NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A PROTOTYPE RULE BASED SYSTEM FOR
ELECTRONIC WARFARE

by

Hsiung, Wen-Cheng

June 1991

Thesis Advisor: Yuh-Jeng Lee

Approved for public release; distribution is unlimited.

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY 2b DECLASSIFICATION / DOWNGRADING SCHEDULE	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; Distribution is unlimited
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (If applicable) 3A	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)

A PROTOTYPE RULE BASED SYSTEM FOR ELECTRONIC WARFARE

12 PERSONAL AUTHOR(S)

Hsiung, Wen-Cheng

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM ________ TO ______	1991 June	83

16 SUPPLEMENTARY NOTATION

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defence or the U.S. Government

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Electronic Warfare, Functional recognition, Artifical Intellignce, Expert system, Rule-based system.

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This thesis examines the feasibility of using an expert systems to solve the threat identification problem in the radar signal environment. Such systems can be used to support the Electronic Warfare Officer (EWO) in decisions-making. We have analyzed the expertise required in electronic warfare (EW) and have identified key signal parameters. In addition, we have devised a method called function recognition to facilitate radar signal analysis.

A rule-based prototype system possessing EW knowledge has been designed and developed for a micro-computer system using the expert system shell CLIPS. The system is able to receive preprocessed sensor inputs, determine the radar signals that are present, perform threat target identification, and suggest the best possible electronic counter measures.

The behavior of the system is demonstrated using several hypothetical EW scenarios. We believe that such a system can be incorporated as an electronic warfare (EW) subsystem.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION
22a NAME OF RESPONSIBLE INDIVIDUAL Yuh-Jeng Lee	22b TELEPHONE (Include Area Code) (408) 646-2361 22c OFFICE SYMBOL CS/Le

DD Form 1473, JUN 86 Previous editions are obsolete. SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603 Unclassified

A Prototype Rule Based System For Electronic Warfare

by

Wen-Cheng Hsiung
Lieutenant Commander, Republic of China Navy
B.S., Chinese Naval Academy, 1980

Submitted in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 1991

ABSTRACT

This thesis examines the feasibility of using an expert system to solve the threat identification problem in the radar signal environment. Such systems can be used to support the Electronic Warfare Officer (EWO) in decision-making. We have analyzed the expertise required in electronic warfare (EW) and have identified key signal parameters. In addition, we have devised a method called function recognition to facilitate radar signal analysis.

A rule-based prototype system possessing EW knowledge has been designed and developed for a micro-computer system using the expert system shell CLIPS. The system is able to receive preprocessed sensor inputs, determine the radar signals that are present, perform threat target identification, and suggest the best possible electronic counter measures. The behavior of the system is demonstrated using several hypothetical EW scenarios. We believe that such a system can be incorporated as an electronic warfare (EW) subsystem.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

This study would not have been possible without my thesis advisor, Professor Yuh-jeng Lee, who provided both encouragement and the professional knowledge for this study. Within the area of electronic warfare, Professor Donald v. Z. Wadsworth, my second reader, was also very helpful in this study.

Finally, to my wife – Chia-Hui, and my daughter – Pei-Yu, thanks for their loving support and patience during the writing of this thesis.

I. INTRODUCTION

A. BACKGROUND

Electronic warfare equipment was developed to achieve operational objectives. From a tactical point of view, the key role of electronic warfare is to intercept the enemy radiated signals to obtain two elements of tactical information, i.e., warning and identity. Characteristic signal parameters, such as radio frequency, pulse width, pulse repetition rate and scan rate, are required to gain this information. They constitute a form of diagnostic signature that identifies the signal emitter that can be compared with intelligence information on enemy signal characteristics.

The most important tactical information obtained from the interception of enemy signals is that relating to target identity which results from analysis of the signal characteristics. Signal analysis is such an important feature for evaluating target identity that all modern ESM equipment can be programmed to recognize and give immediate warning of nominated, specific threat radars which pose potential dangers requiring very quick reaction.

The basic requirement of ESM equipment, when used for target identification, is fast response and accurate identification. Of course, any automatic ESM equipment will fail in the target identification process when the intelligence library contains insufficient data. Also, during combat, the response to a threat must be in real-time to maintain the safety of the Naval vessel. Therefore, producing a fast response and correct identification are vitally important.

Expert systems have been successfully constructed for a wide range of applications such as speech recognition, medical diagnosis, and signal processing. It

is desirable to apply the expert system technology to electronic warfare to perform target identification, which is aimed at assisting the Electronic Warfare Officer (EWO) in critical operations of a threat environment. In a high density threat signal environment, the EWO must make major electronic counter measure decisions in response to an enemy signal interception. An example of such a decision is whether or not the threat signal should be jammed and the procedure to use to jam the signal. The EWO must make a correct decision in an extremely time-critical and high-pressure situation and select the appropriate ECM to ensure effectiveness. The augmentation of the EWO's personal experience into an expert system would be a valuable tool to help the EWO respond quickly to a wide variety of adverse situations.

B. PROBLEM

The reasons for using an expert system to aid target identification and decision making in EW include:

- Reducing the response time in manual target identification based on table look-up from an Electronic Parameter List (EPL), for ships not equipped with an automatic ESM system.

- Backing up existing automatic ESM systems that evaluate threat signals against an EPL. This EPL database is limited to those signals collected from intelligence; when a signal cannot be identified in the database, the system fails.

- Enhance the performance of the less experienced EW personnel.

C. GOALS AND OBJECTIVES

This thesis attempts to design and develop a "rule-based" expert system prototype for target identification, by encoding the expertise of the decision making process in the area of electronic warfare.

The system receives preprocessed sensor input, determines what radar signals are present, performs threat identification, and suggests the best possible electronic counter measure to take.

The goal of this developmental effort is to determine the feasibility and suitability of using an expert system to improve the threat identification capability of systems currently used aboard naval ships.

D. SCOPE

This thesis will only be concerned with using a rule-based system to perform threat identification and to aid the EWO in arriving at the best decision. It is not aimed at the development of a complete, automatic ESM system.

The term "threat" is used extensively throughout this thesis. The threats comprise different kinds of radars. Additionally, to analyze all of these radar performance characteristics, jamming effectiveness, and to do threat signal analysis is beyond the scope of this thesis. In developing a rule-based program which involves threat signal parameters of interest, this thesis will not include classified parameter material. The unclassified data used to support the thesis program are based on fictitious data. Any unclassified information about the threat was obtained from the open literature.

The discussion above illustrates the need for using an intelligent expert system to aid the decision making process. This process consists of three phases: acquisition, analysis and display. In the acquisition phase, the expert system receives signal

parameters from the various ESM equipment and intelligence sources and stores that information in a dynamic database. In the analysis phase, the expert system scans its database for possible correlations and performs the necessary calculations to verify the correlation. In the display phase, the expert system indicates target identifying information and suggests the best possible ECM to supplement the EWO's decision-making process.

The remainder of the thesis is organized as follows: Chapter II analyzes the EW basis signal parameters of interest. It also includes discussions on some functional recognition methods which are incorporated in the expert system. Chapter III defines an expert system structure and discusses the development of the rule-based system. Chapter IV discusses the EW rule-based system program, with examples showing the behavior of the prototype. Chapter V presents the conclusions arrived at in this thesis.

II. EXPERT KNOWLEDGE OF ELECTRONIC WARFARE

A. DEFINITION

Electronic warfare (EW) is an indispensable type of combat which directly relates to the tremendous progression of electronic technology and has influenced the characteristics of warfare to the point that this type of combat is essential in today's conflicts. According to Schleher [Ref. 1], the purpose of EW is to exploit the enemy's electromagnetic emissions in all parts of the electromagnetic spectrum in order to provide intelligence on the enemy's order of battle, intention, and capabilities, and to use counter measures to deny the enemy's effective use of communication and weapons systems while protecting one's own effective use of the same spectrum. Even when engaged in relatively simple military operations, there are advantages to be gained from the use of electronic warfare capabilities.

The definition of electronic warfare is that division of the military employment of electromagnetic energy involves actions taken to determine, exploit, prevent, or reduce an enemy's effective use of radiated electromagnetic energy. Electronic warfare has three main subdivisions: electronic support measure (ESM), electronic counter measure (ECM), and electronic counter-counter measure (ECCM). Figure 2.1 indicates the relationships between these three elements. The ESM intercepts the enemy tactical information for the purpose of threat recognition and for selecting the appropriate ECM against the enemy's tactical actions. In addition, it also suggests the ECCM to be taken to defeat the enemy's tactical action.

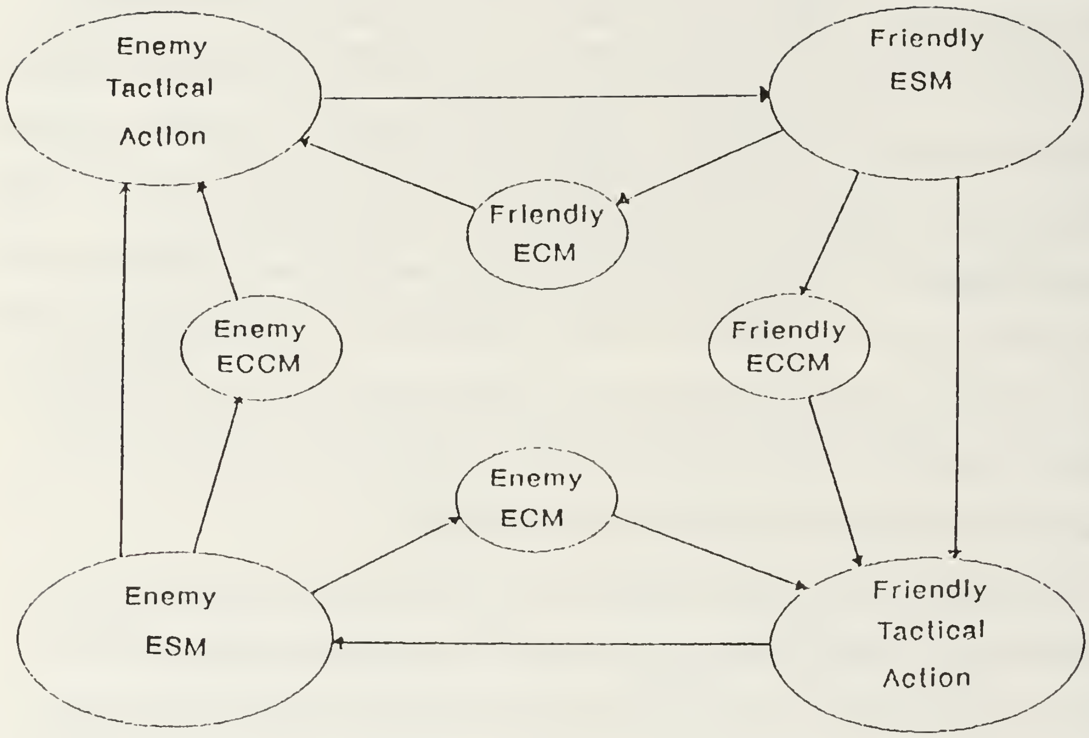

Figure 2.1: The Interactions of ESM, ECM, and ECCM

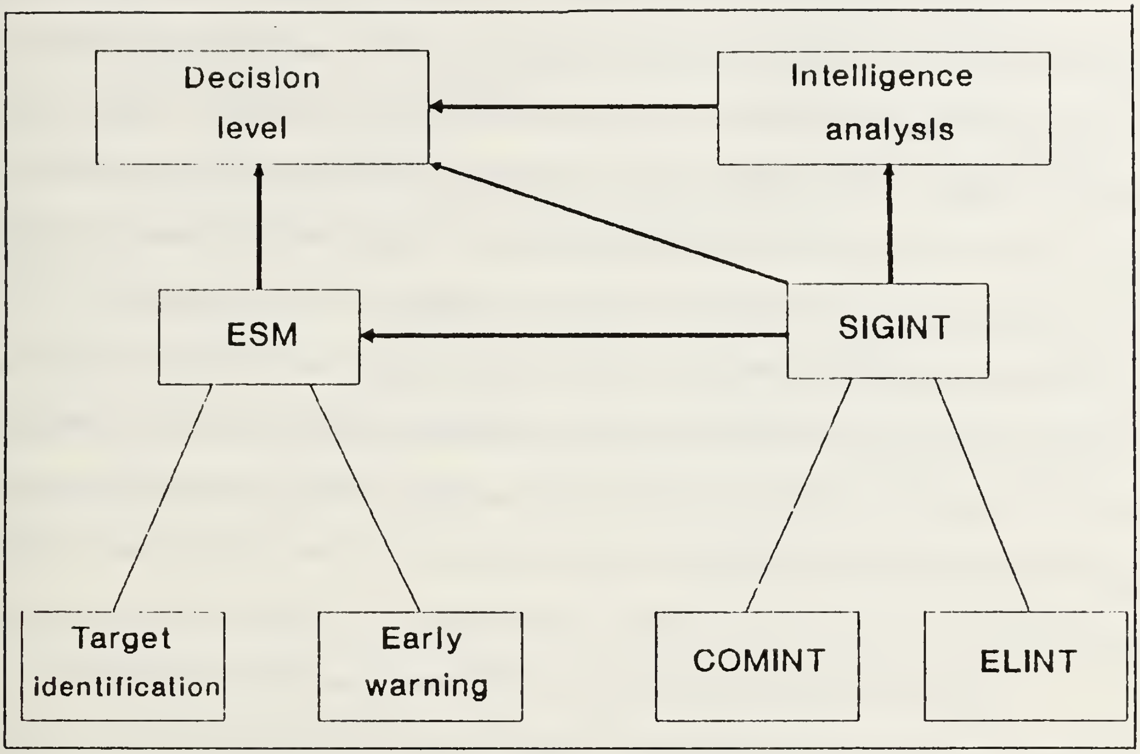

Figure 2.2: Relationship Between ESM and SIGINT

1. Electronic Support Measures (ESM)

ESM is defined as the actions taken to search for, intercept, locate, and immediately identify radiated electromagnetic energy for the purpose of immediate threat recognition and the tactical employment of forces [Ref. 1]. Thus, ESM provides a source of EW information necessary to conduct ECM, ECCM, and threat identification. A similar function of ESM is known as signal intelligence (SIGINT). SIGINT is a generic term that includes both communication intelligence (COMINT) and electronic intelligence (ELINT). The difference between the ESM function and the SIGINT function is that ESM focuses on tactical functions and SIGINT is based on strategic functions. Figure 2.2 indicates the relationship between ESM and SIGINT.

The EW systems used for ESM and SIGINT are similar. The difference is that the information obtained from the ESM is directly accessible to the decision level, whereas with SIGINT the information access can be either directly or indirectly related to the decision level. The efforts of SIGINT can also be used to support ESM. For example, the ESM system can classify the threat signal, due to the internal programmable library in which parameters are required from SIGINT to establish the database. SIGINT has two subdivisions, one of which is ELINT. ELINT's function is to identify the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information concerning foreign nations or areas of operation. Important collection of radar signal parameters or other signals can be performed during peacetime.

There are many different types of ESM systems which vary greatly in functional performance characteristics. ESM systems can operate in a very dense electromagnetic environment. If a signal is detected, its parameters are determined and identification can be an automatic operation performed as it is received. In many situations, the available defensive reaction time is short, therefore, automatic signal search and recognition without human aid is necessary. An example is a radar warning receiver (RWR) used in special mission attack platforms that alerts the commanding officer of detection by enemy tracking radar. RWRs accomplish this by sensing the signals from threat radars, providing an audio warning signal, and displaying the warning information on a video screen. All the information includes either the location or the relative bearing and rank of the threats, in order of danger, to the commanding officer. Disadvantages of the ESM system depend on the type of ESM receiver used. For example, in a high signal environment, a tunable RF crystal video receiver (TRFCVR) can be saturated more easily than other types of ESM receivers. Because the TRFCVR has a narrow bandwidth, the receiver has

a slow response time for covering a wide frequency range. Another example is the superheterodyne receiver, which tunes the frequency at any tuning position in a narrow band. It is much more selective and is less susceptible to saturation in a dense signal environment. However, tuning over the total frequency range takes a certain amount of time and signals of interest might be missed.

ESM has several advantages, one of which is that ESM operates in a completely passive mode. ESM does not radiate electromagnetic energy, and thus is capable of detecting threats before the threat is capable of detecting the target. In general, the ESM detection range can be much greater than the radar detection range. Two methods can be used to calculate the ESM detection range, power comparison or line-of-sight.

In power comparison, the ESM maximum detection range is affected by many factors, such as ESM receiver sensitivity, emitter antenna gain, power, etc. Equation 2.1 describes this factor relationship. Equation 2.2 indicates the maximum detection range of the ESM receiver.

$$P_r = \frac{P_t \times G_t \times G_r \times \lambda^2 g^2}{(4\pi R)^2 L_p \times L_s} = S_{min} \tag{2.1}$$

$$R_{max} = \sqrt{\frac{P_t \times G_t \times G_r \times \lambda^2 g^2}{(4\pi)^2 \times S_{min} \times L_p \times L_s}} \tag{2.2}$$

where

- P_r = power received by the ESM receiver
- P_t = emitter power
- G_r = ESM antenna gain
- G_t = emitter antenna gain

- λ = emitter wavelength
- g = propagation factor
- R = distance between emitter and ESM receiver
- R_{max} = maximum detection range of ESM receiver to detect emitter sidelobe
- S_{min} = ESM receiver sensitivity
- L_p = propagation loss
- L_s = system loss

Assume the emitter transmitter power is 100 kW with a frequency of 12 GHz, the emitter antenna gain is 30 dB, the ESM antenna gain is 30 dB, the ESM system sensitivity is -94 dBm, and the propagation loss between the emitter and the ESM receiver is 3 dB. The maximum detection range of such an ESM system is about 300 km. The effective ESM detection range can be subject to severe line-of-sight (LOS) constraints. Because of the curvature of the Earth (Figure 2.3), there is a limiting distance at which an ESM antenna has an unobstructed view of the transmitting antenna. Figure 2.3 shows the case of a smooth earth path. According to Griffiths [Ref. 2], the ESM maximum detection is calculated by using Equation 2.3.

$$d = 4.12(h_t + h_r) \tag{2.3}$$

where

- d_1 = in ground range from the transmitter (Figure 2.3)
- d_2 = in ground range from the receiver (Figure 2.3)
- d = the ground range between the transmitter and receiver in km

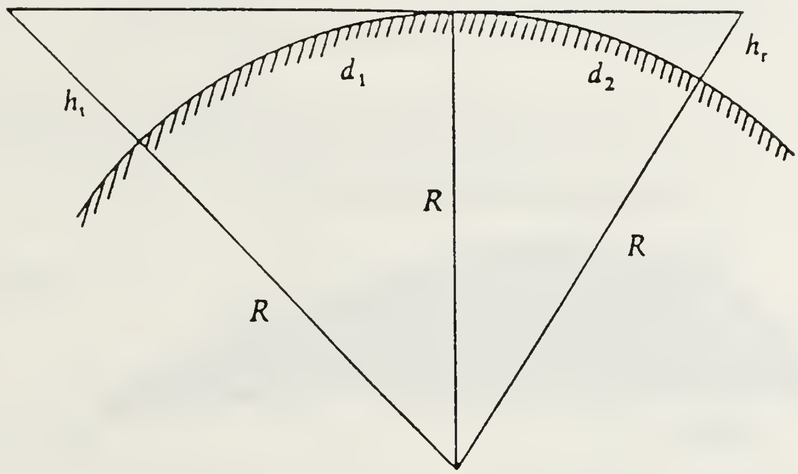

Figure 2.3: ESM Detect Range Limited by Earth Curvature Effect (This figure reproduced from Radio wave propagation, J. Griffiths, 1987, pg. 100)

- h_t = the heights of the transmitting antennas in meters
- h_r = the heights of the receiving antennas in meters
- R = the effective radius of the earth, R=8500 km

If both transmitting antenna and receiving antenna are at the same height of 100 m, the maximum detection range of the ESM receiver is 82.4 km.

Although the ESM detection range can be much greater than the radar detection range, in practical situations (due to the Earth curvature effect), when the ESM detects the presence of a signal from the enemy radar, it may be assumed the enemy site has made radar contact with the ESM ship. Figure 2.4 indicates a typical ESM detection range geometry [Ref. 3].

2. Electronic Counter Measures (ECM)

The primary objective of ECM is to deny the use of the electromagnetic spectrum to the enemy forces in order to allow our own military force to complete

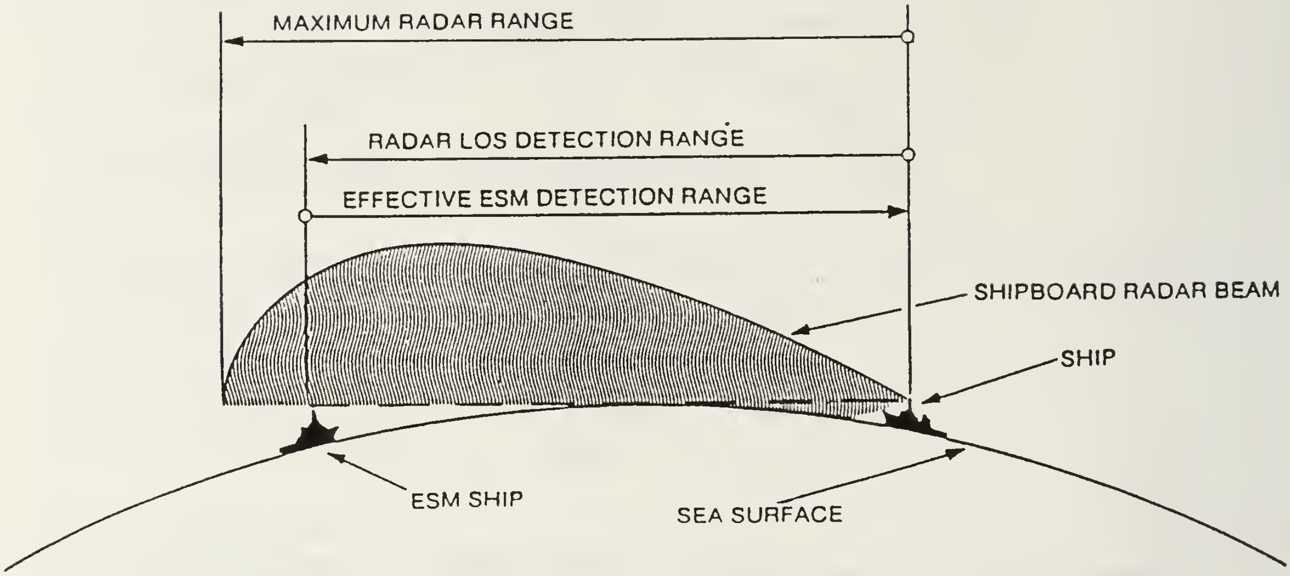

Figure 2.4: Typical ESM Detection Range Geometry (This figure reproduced from ICH, 1980, p. 361)

its mission successfully. ECM is defined as actions taken to prevent or reduce the enemy's effective use of the electromagnetic spectrum [Ref. 1]. There are four types of ECM tactics employed in the EW world, i.e., self-screen jamming (SSJ), standoff jamming (SOJ), standforward jamming (SFJ), and escort jamming (EJ). In SOJ, the jamming platform remains close to but outside of the lethal range of the enemy radar missile system. In escort jamming, the jamming platform accompanies the friendly strike vehicles. In standforward jamming, the jamming platform is positioned between the enemy radar missile systems and the friendly strike vehicles [Ref. 4]. Self-screening jamming is an ECM technique in which a military vehicle carries a jammer and an off-board jammer launching system, used to protect itself from threatening enemy electronic systems. In this thesis, a rule-based system is used to support the electronic warfare officer (EWO) to allow for the best decisions

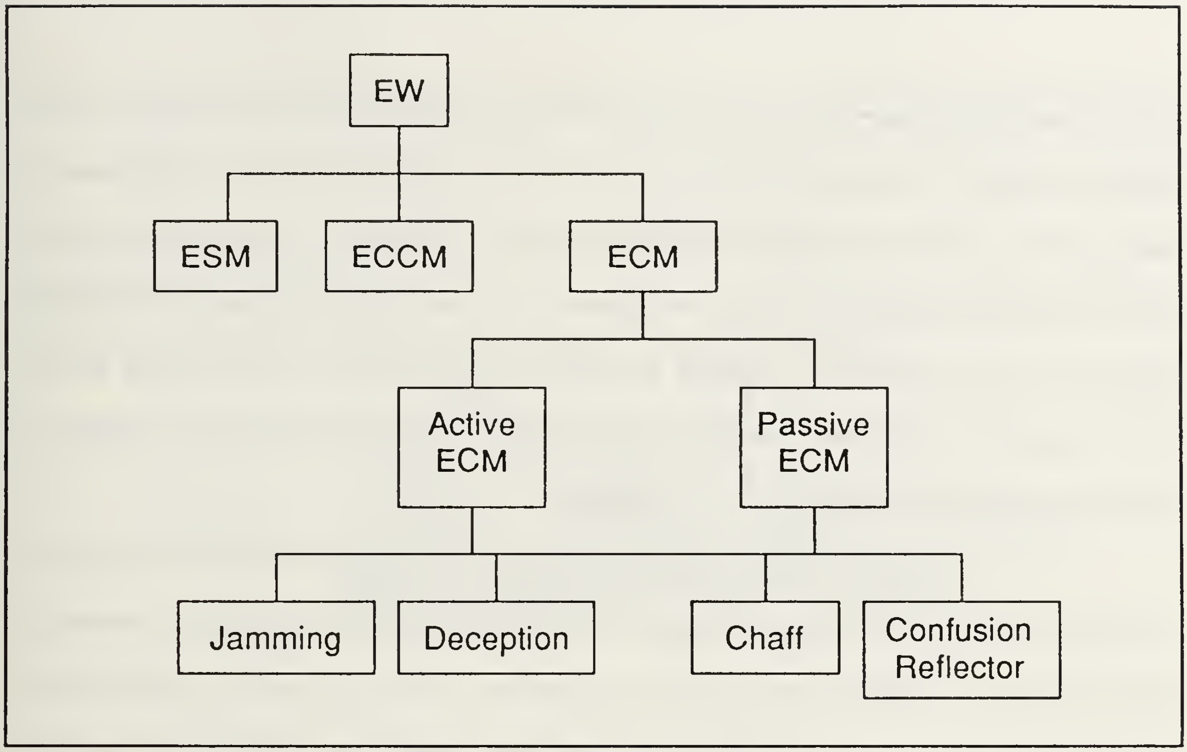

Figure 2.5: Area of ECM

based on the SSJ. Therefore, the knowledge of ECM SSJ concepts as related to the expert knowledge of EW are briefly discussed in this section.

ECM has two principal areas: active ECM and passive ECM. Active ECM includes noise jamming and deception, whereas passive ECM includes chaff and confusion reflectors. The active ECM is the deliberately generated and radiated radio frequency signals given to compete with true radar reflected signals to disrupt the intended function of the victim radar or missile. The passive ECM are the devices designed to reflect the intercepted radar radiation so that the reflections compete with true target returns and conceal the true target position. Figure 2.5 represents the area of ECM.

a. Jamming

Jamming is an ECM technique used to deny an enemy use of an electronic system. Jamming is best described as the deliberate radiation or reflection

of electromagnetic energy to the enemy's defense system so that the system is not able to extract true data. Noise jamming is the most common form of ECM and is performed in two basic modes - SPOT and barrage. The basic concept for these two types of noise jamming are shown in Figure 2.6. In a SPOT jamming, the jammer must be set onto the threat emitter frequency and must focus the jamming power into a narrow bandwidth. The bandwidth should be made as narrow as possible to obtain the maximum power per unit bandwidth.

In the EW world, modern radar employs frequency agility to improve jamming resistance. Frequency agility is the ability of radar to change its operation frequency to be effective against SPOT jamming. Since the radar's bandwidth is increased when the frequency is changes, it will not be efficient in SPOT jamming. In order to overcome uncertain frequency parameters, barrage jamming may be used. A barrage jammer requires considerably more effective radiate power (ERP) than a SPOT jammer to achieve the same jamming effectiveness [Ref. 1]. Therefore, the power of the jamming signal is actually less than for SPOT jamming when insufficient power is used in barrage. This phenomenon is illustrated in Figure 2.6. For example, if a jammer ERP is 50 kW and the bandwidth is 5 MHz for SPOT jamming and a wider bandwidth is 500 MHz for barrage jamming, the maximum jammer power in a given bandwidth is $\frac{50\ kW}{5\ MHz} = 10\frac{kW}{MHz}$ and $\frac{50\ kW}{500\ MHz} = 0.1\frac{kW}{MHz}$ for barrage jamming.

ERP is defined as the product of the transmitted power and the antenna gain. While a high ERP is desirable, the use of a very high-gain antenna may cause disadvantages in this method. A very high-gain antenna implies a very narrow beam. It may be difficult to keep such a narrow beam on the victim if the victim is moving rapidly. Also, a very narrow beam might not permit simultaneous jamming of several victims located in the same area. Jammer power requirements

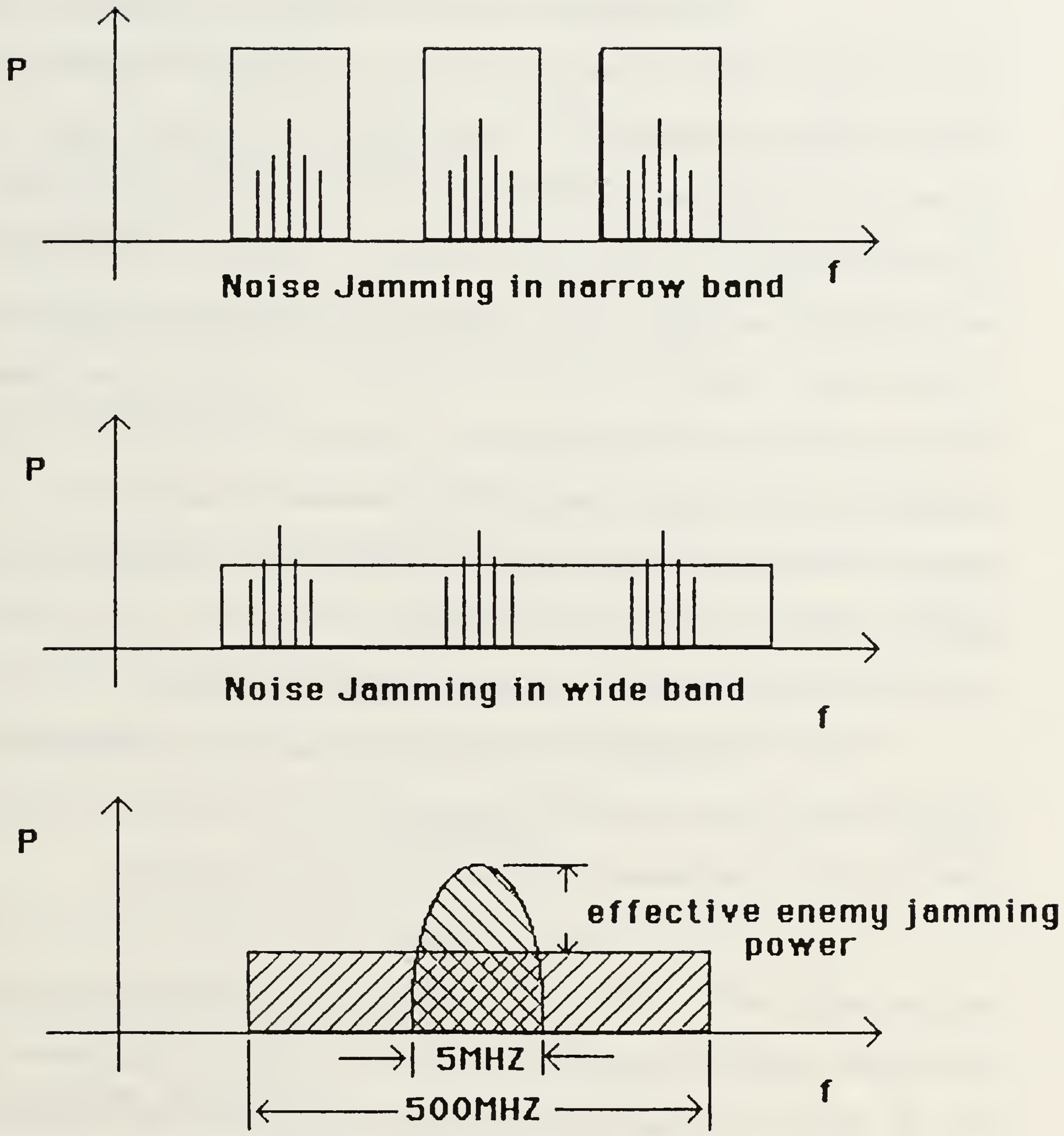

Figure 2.6: SPOT Jamming and Barrage Jamming

should include the consideration of two aspects, radar sidelobe jamming and the jammer to signal power ratio, J/S.

(1) Sidelobe Jamming

Low sidelobes are generally desired for radar systems. However, antenna designers prefer to design radar systems with a high mainlobe and lower sidelobe antennae. Otherwise, if a large portion of the radiated energy were to concentrate in the sidelobe, a reduction in the main-beam energy would occur with a consequent reduction in radar system sensitivity. According to Skolnik [Ref. 5], if the sidelobe levels are higher, a strong echo signal could enter the receiver and appear as a false target. Jamming via the radar sidelobe can result in serious degradation of radar performance as the radar pattern is composed of the mainlobe and several sidelobes into which noise is received. This can result in the indication of strong echoes on the radar plan position indicator (PPI), making it difficult for the radar operator to extract correct target information.

(2) Self Screen Jam-to-Signal Ratio (J/S)

In practical ECM jamming systems, it is desirable to understand the fundamental relationship between the J/S ratio required at the victim's receiver to remain undetected and the noise quality of the jammer.

The J/S radio is defined as the relationship of the effective jamming signal power in the victim electronic system bandwidth to the desired signal power. Both are measured at the same place and time in the jammed receiver [Ref. 4]. To get an estimate of the necessary power required for the jammer, the following calculations are used.

$$\begin{aligned} S &= \frac{P_t \times G_r}{4\pi \times R^2} \times \frac{\rho}{4\pi \times R^2} \times \frac{G_r \times \lambda^2}{4\pi} && (2.4) \\ &= \frac{P_t G_r^2 \rho \lambda^2 F^4}{(4\pi)^3 R^4} && (2.5) \end{aligned}$$

where

- S = received echo signal power
- P_t = radar power output
- G_r = radar antenna gain
- ρ = radar cross section of a target
- λ = wavelength
- R = distance between radar and target
- F = propagation factor

A non-free-space environment will change the E field arriving at the receiving antenna. The component E picked up by the receiving antenna can be different from that in a free-space situation, E_o. The ratio $\mid \frac{E}{E_o} \mid$ is called the propagation factor. The propagation factor in the equation above illustrated two-way propagation, e.g., F^4. Jammer power in the receiver bandwidth is:

$$J = \frac{P_j G_j B_r G_r \lambda^2 F^2}{(4\pi)^2 R^2 B_j L_p} \tag{2.6}$$

where

- J = Jammer signal power at radar
- P_j = Jammer power output
- G_j = Jammer antenna gain
- B_r = Radar bandwidth
- G_r = Radar antenna gain (sidelobe)

- λ = Wavelength
- R = Distance between jammer and radar
- B_j = Jammer bandwidth
- L_p = Polarization loss
- F^2 = Propagation factor (one way propagation)

The jammer uses a "slant" antenna or circularly polarized radar. In either case, L_p is 2 for horizontally or vertically polarized radars [Ref. 6].

By combining Equations 2.5 and 2.6, we obtain a jam-to-signal ratio.

$$\frac{J}{S} = \frac{P_j G_j B_r 4\pi R^2}{P_t G_r B_j \rho L_p} \tag{2.7}$$

$$= \left(\frac{P_j G_j}{P_t G_r}\right)\left(\frac{B_r}{B_j}\right)\left(\frac{4\pi R^2}{\rho L_p F^2}\right) \tag{2.8}$$

Equation 2.7 can be used to find the power required of a jammer. For example, assume J/S is 0 dB for noise jamming, radar frequency is 8 GHz, the radar polarization is horizontal, the radar ERP is 250 mW, the BW is 5 MHz, the jammer antenna gain is 20 dB with BW of 100 MHz, the attack boat RCS is 10 m^2, the jammer ship RCS is 20,000 m^2, the distance between the jammer and radar is 30 nm, the propagation factor is 0 dB, then

$$1 = \frac{P_j \times 100 \times 5\ MHz\ \times 4\pi \times 3.24 \times 10^{10}}{250 \times 10^6 \times 100\ MHz\ \times 20000 \times 1.99} \tag{2.9}$$

$$P_j = \frac{250 \times 10^6 \times 100 \times 20000 \times 1.99}{100 \times 5 \times 4\pi \times 3.24 \times 10^{10}} \tag{2.10}$$

$$= 4.9\ W/MHz \tag{2.11}$$

From the calculation, the minimum power required for the distance of 30 nautical miles is about 4.9 W/MHz.

b. Deception

Deception is defined as the deliberate radiation, reirradiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead a hostile force in the interpretation or use of information received by its electronic system [Ref. 1].

The objective of deception is to provide a means of protection against radar systems. Protection is accomplished by using deceptive amplified and repeated pulsed RF signals received from a threat radar. This is different from noise jamming which tries to overwhelm the radar systems with noise, making the extraction of the real data difficult. However, noise jamming is not an appropriate technique for tracking radar [Ref. 1]. One reason is that the tracking radar requires azimuth, elevation, and range to determine the present target position, therefore, the noise signal which allows the fire control or missile guidance system for calculation or correlation processing. A second reason is that noise jamming can only deny range information and not angle information. If the power of a noise jammer is not enough when the noise signal goes into the main lobe, the radar operator can still get azimuth information.

A significant advantage of deception jamming is that the power required is less than noise jamming. Since the noise jamming is operated in almost 100% of the duty cycle, peak power equals average power. The deception jammer generating the pulse is matched with the radar's pulse, operating at a duty cycle equal to that of the tracking radar.

One example of deception jamming is known as range gate pulloff (RGPO). Tracking systems use range gates to detect the range of a target echo. The gates are adjusted by the tracking system in order to keep radar tracking efficient. The objective of the range deception jammer is to steal the gate by forcing the

gate to a position other than the true echo. This range gate pulloff technique is commonly employed. The RGPO function is accomplished via the interaction of the radar and deception jammer. The deception jammer is a repeater that is always triggered by radar pulse. The pulse is retransmitted with the same width but a higher amplitude back to the radar to capture the radar automatic gain control circuit. Once the gate is completely in the pulloff stage, the repeater turns off, causing the true target to disappear from the tracking system. During this period the target range information is incorrect with the degree of range error depending on the pulloff time. The maximum time is generally about 20 μs and could cause a distance error of as much as 3200 yards.

c. Passive Electronic Countermeasure

(1) Chaff

Chaff is the oldest and one of the most widely used radar countermeasures [Ref. 1]. Chaff is an intentional clutter generator, consisting of quantities of radar reflecting material. Such large quantities of reflecting material can produce significant clutter, saturating threat systems and providing false targets, thereby confusing a radar operator. Chaff is a collection of small segments of aluminum foil cut to lengths of approximately one-half the wavelength of the radar frequency band of interest.

For naval applications, the purpose of chaff is to provide self protection and to provide false targets to confuse the threat radar with false information. The effectiveness of chaff depends on the current situation and its intended use. If an outside intelligence source is unavailable, the ship must operate independently and relies on its own ESM system or radar. Radar is an active sensor limited by the emission control (EMCON) policy. Therefore, most early warning information is derived from the ESM system. Additionally, since the purpose of the chaff

is to provide self protection from missile attack or to confuse the radar operator, appropriate action tactics should be considered in the decision-making effort before firing. Figure 2.7 illustrates the proper procedure in a period of war.

Two major factors are considered when determining the appropriate time for firing the chaff, the seeker activating range from the ship and the chaff cloud forming time. For example, if the activated seeker is 10 nautical miles away, the chaff's units will burst open and form a cloud in approximately 15 seconds, if the missile speed is 250 m/sec, the chaff will produce the lock transfer function at 14 seconds if the chaff is fired at 14 nautical miles. However, a missile seeker is generally activated much closer to a target ship. If the chaff is still fired at 14 nautical miles for a missile seeker activated at 6 nautical miles away from the ship, the lock transfer function of a chaff will not be effective since the missile seeker has its own operational characteristics.

A discussion of missile seekers is beyond the scope of this thesis.

(2) IR Flare

The purpose of using an IR flare is to guard against an IR seeking missile. The IR seeker provides the information to position a target for the missile system. The IR seeker can lock onto a ship's smoke stack exhaust gases, as the gases provide a large transmittance. Radiation is emitted in the 3-5 μm IR region with its contribution of heat radiation area at about 20 m^2. The difference of contrast between the ship's temperature and its own background temperature is the determinant factor for the success of an IR guided missile. At a large distance, the ship acts as a point source if a flare is fired. However, the flare has more thermal power than the ship and the missile is thus distracted by the IR flare. As the temperature of the flare decreases, its effectiveness decreases as it radiates out of the IR region. At this time, the IR seeking missile has a greater probability of

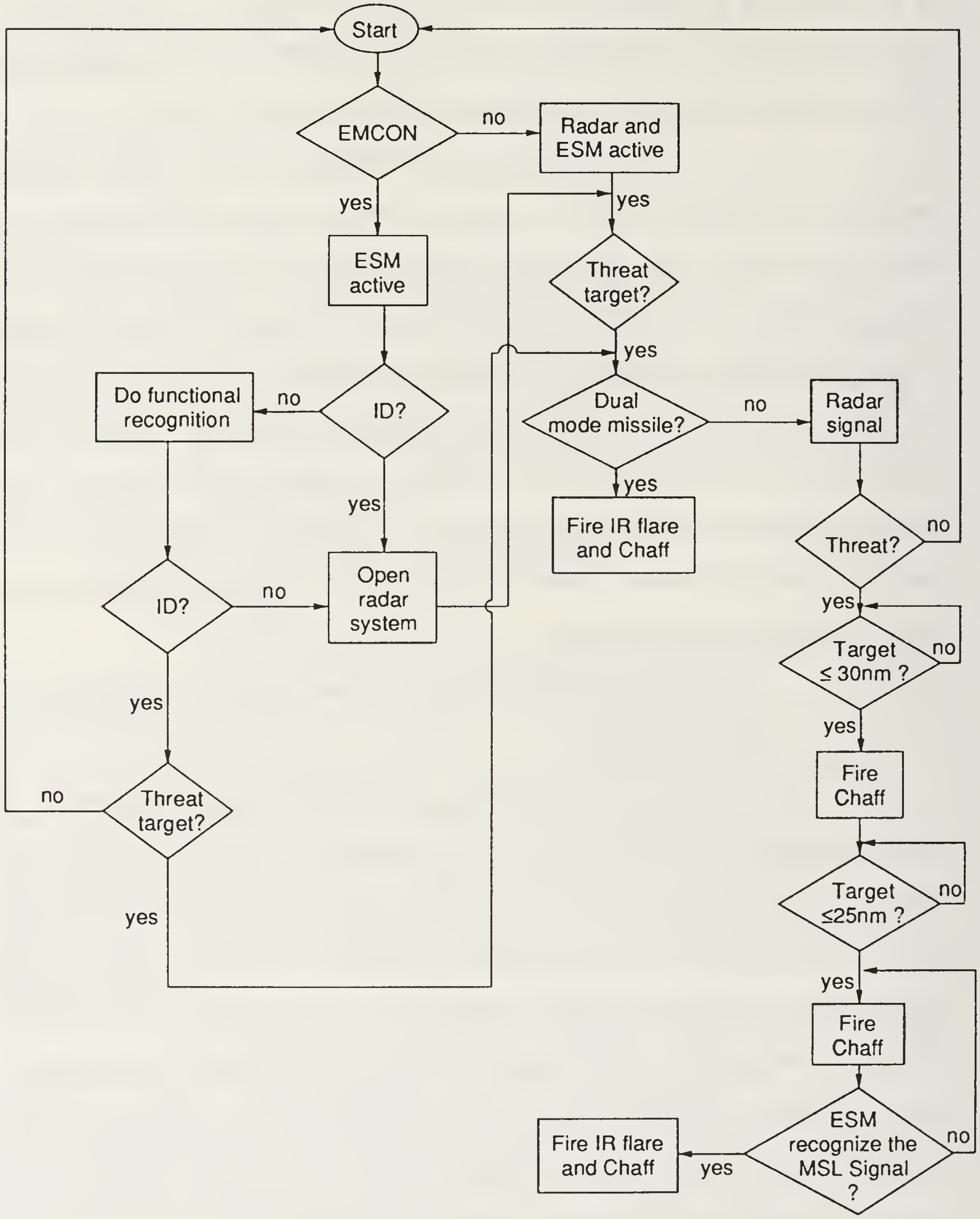

Figure 2.7: A Basic Procedure for Firing a Chaff and IR Flare

locking onto the ship's radiation area and could result in the missile centroid mode. To protect the ship from the IR seeking missile, the IR flare should be fired when the missile signal is intercepted by the ESM system as early as possible to avoid missile centroid mode.

B. KNOWLEDGE OF THREAT SIGNAL PARAMETERS

The purpose of the intercepted signal is to locate the enemy emission source position and to identify the threat signal. The most important tactical information that can be obtained from an intercept of enemy signals relates to target identification by the analysis of the signal characteristics [Ref. 7]. An EW operator must be able to operate the ESM system efficiently to support decision making, but the ESM system must be able to intercept the signal and accurately process the many parameters from the emitter. The principal radar parameters of interest are frequency, pulse width (PW), pulse repetition frequency (PRF), scan rate, modulation type, PRF stability, etc. Unfortunately, in today's high density electronic environment, different electronic systems have closely similar parameters. Parameters of systems associated with a generic threat vary somewhat from system to system causing ambiguous identification. Deep analysis of signal parameters is beyond the scope of this thesis, but the most important concept of signal parameter characteristics is related to expert knowledge of EW, as discussed in this section.

1. Frequency

Since electromagnetic waves propagate in air with oscillations occurring at different rates, a frequency is defined as the number of cycles of the signal oscillation observed at any point in the signal per unit time. In the EW field, the necessary measure of frequency is the carrier frequency of a signal. The determination of carrier frequency provides valuable information which can aid target

recognition. If the carrier frequency is measured, an approximation of the evaluation of the target can be identified. Basically, a lower frequency indicates a larger antenna, higher power, higher gain, narrow beam and longer detect ranges. Higher frequencies indicate a smaller antenna, lower power, lower gain, wider beamwidth, higher doppler response, and shorter detection range. There are some limitations to be aware of when measuring carrier frequency. The accuracy of radio frequency (RF) measurement is subject to many variables, as listed below [Ref. 7]

- The accuracy of the available frequency standard.
- The available signal-to-noise ratio for single pulses and the ability of the receiver system to integrate a number of pulses.
- Doppler shifts due to motion of the emitter or the receiver.

The ability to measure frequency depends on the ESM receiver performance and EW operator training. The EW operator is important because the EW operator introduces a human factor, reflected by coordination with the ESM equipment and its functional operation.

Another important effect that should be considered when intercepting frequency is known as the doppler shift. Doppler shift occurs due to motion of the emitter or the receiver, and is defined as the difference in frequency between the transmitted signal and the received signal. When doppler shift occurs, the true carrier frequency needs to be calculated from radar or by other means. The doppler shift frequency calculation between two platforms is given below. [Ref. 7]

$$f_d = \frac{v_r}{c} \times f_o \tag{2.12}$$

where

- f_o = carrier frequency

- v_r = radial velocity

- c = speed of light

- f_d = doppler shift

The doppler shift introduces error in target recognition because of changes introduced in the radio frequency measurement. These changes, up to several kHz, can alter the RF parameters of a radar.

2. Pulse Width

The pulse width (PW) is also called pulse duration. The pulse duration represents the RF energy that was transmitted by the radar in a time period, with the PW defined as the time between the half power points. The envelope of the pulse determines the radar range resolution and also helps to identify the signal type.

Larger PWs indicate large and powerful radars such as those found at landbased sites or on ships. Medium and small PWs are found on ships and aircraft where power generation is limited. Often, modulation products are visible on top of the pulse, aiding in recognition.

These modulation products result from the operating characteristic of the system and display themselves as amplitude variations of the pulse shape (Figure 2.8). The amplitude modulation on pulse (AMOP) could be caused by background clutter, such as mountains. Phase and frequency modulation radars can be identified by looking at their pulses on an oscilloscope. Sometimes, these characteristics are helpful in discriminating between signals with similar parameters. Phase transversal

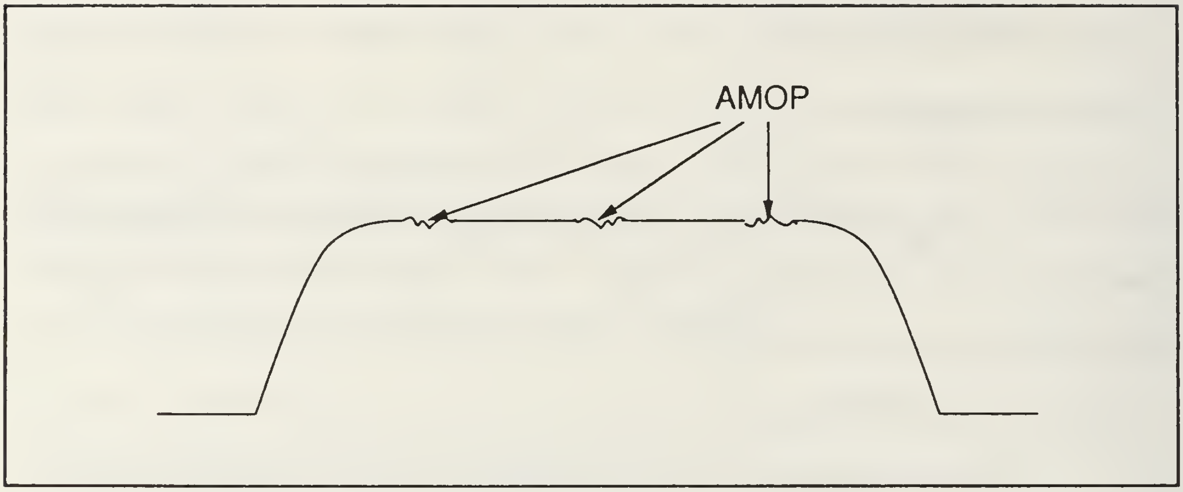

Figure 2.8: Amplitude Modulation on Pulse (AMOP) on an Oscilloscope

(change) is noted by small "glitches" (Figure 2.9) on the pulse, identifying the radar as being phase modulated.

Frequency modulated radars are detected by noting the pulse width as the platform's ESM receiver bandwidth changes. If the pulse width decreases with decreasing bandwidth, the observed air search radar pulse is identified as frequency modulated, or "chirp". If the pulse width remains constant as the bandwidth is varied, no frequency modulation is used. Figures 2.10 and 2.11 demonstrates the concept of measuring the pulse of a frequency modulation radar. Figure 2.12 indicates the CHIRP pulse signal in frequency domain.

By observing the presence of noise (sometimes called grass) on the pulse trailing edge (Figure 2.13), it is possible to determine if the platform's ESM system is in the actual main lobe of the air or surface search radar beam, thereby being within

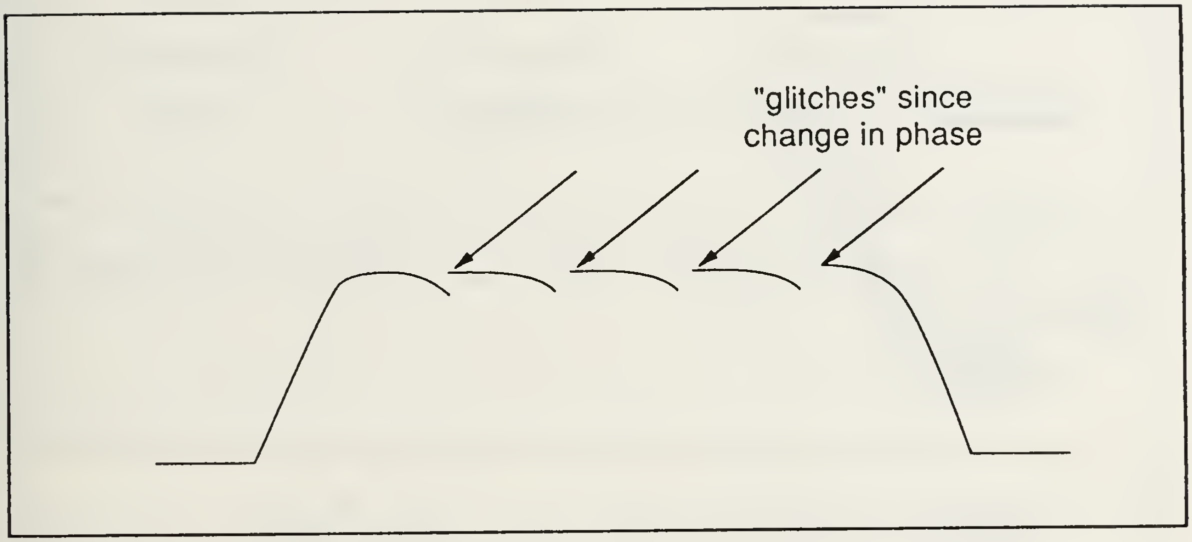

Figure 2.9: Phase Modulation Radar Pulse on an Oscilloscope

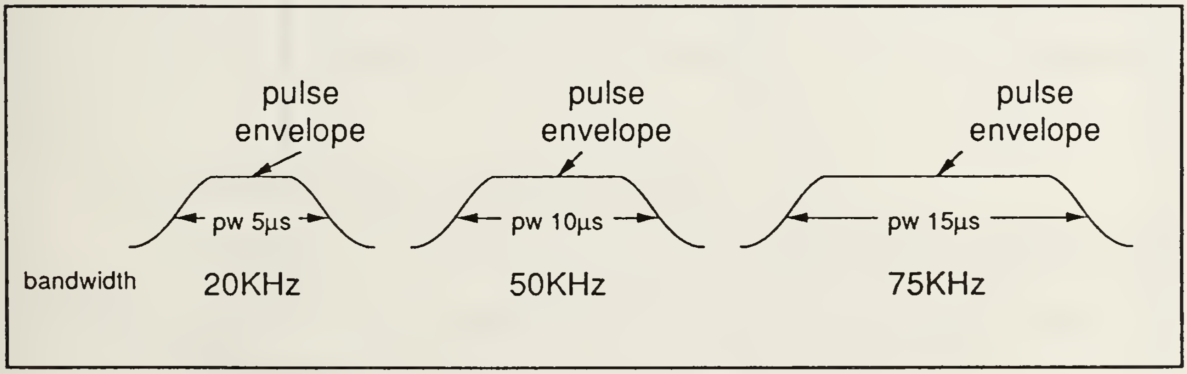

Figure 2.10: Select Different Bandwidths on an ESM Receiver to Identify Frequency Modulation Radar; PW varies with Different Bandwidth selected

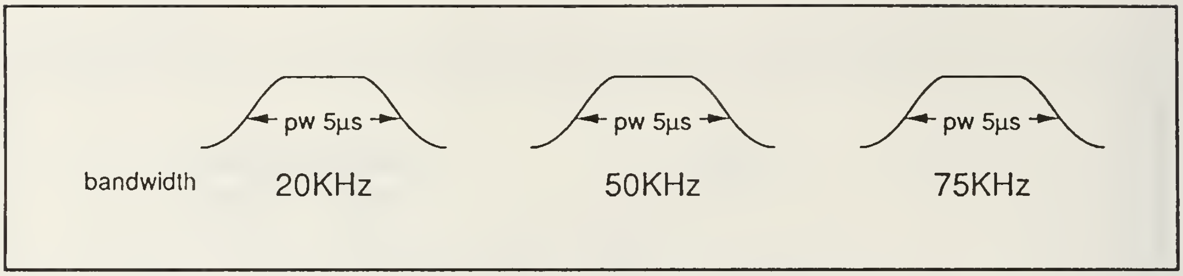

Figure 2.11: PW stays the same when selecting different Bandwidth on an ESM Receiver

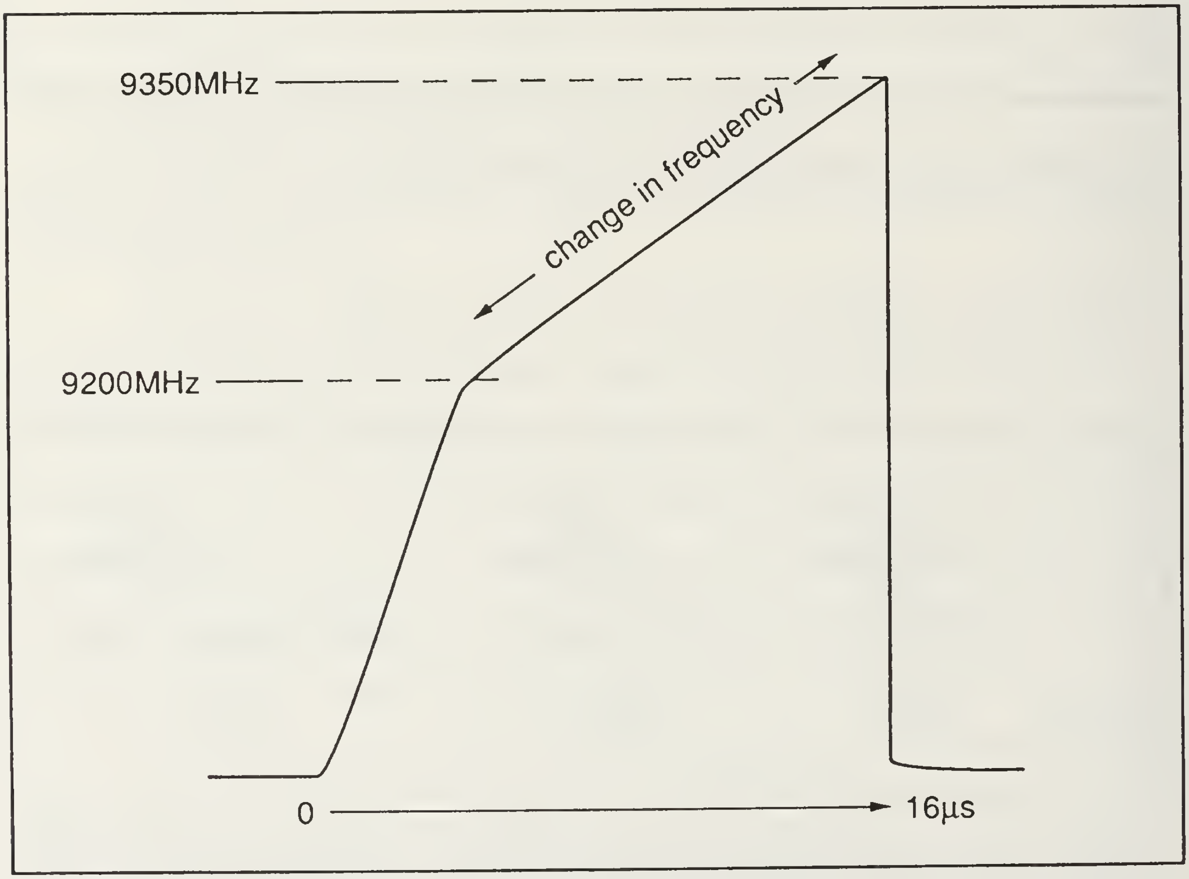

Figure 2.12: Time-Frequency Analyzer Representation of a Chirp Pulse

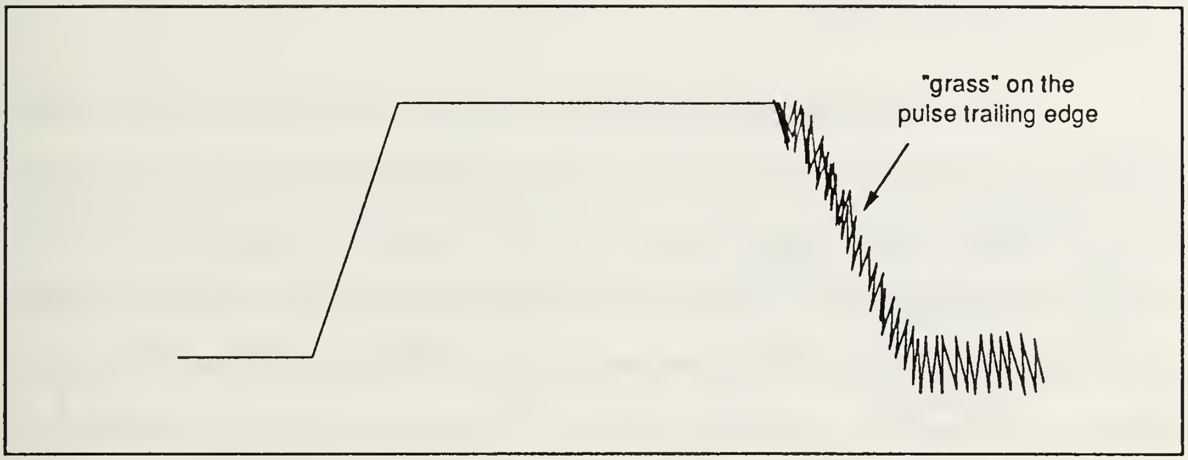

Figure 2.13: "Grass" on the Pulse Trailing Edge Indicates the Aircraft is Detected by the Radar Main Lobe

the detection envelope of the latter. It is often valuable to know the probability of being detected by certain radars.

During air combat, the aircraft uses "penetrate aids" to penetrate a threat radar sidelobe. To prevent the aircraft from being detected by the radar main lobe, the pilot observes the presence of a pulse trailing edge and could take appropriate action.

3. Pulse Repetition Frequency (PRF)

The PRF is an important factor to help the EW operator identify radar performance. One duty is to check the radar's maximum unambiguous range, described by the equation:

$$R_u = c \times \frac{PRI}{2} \,. \tag{2.13}$$

where

- R_u = Maximum unambiguous range
- PRI = Pulse repetition interval
- C = Speed of light

An EW operator can find the radar's maximum detection range by using the PRF parameters of a radar signal. The radar detection range can be calculated by using Equation 2.13. For example, if the ESM receiver's measure of the PRF is 1500 pulses per second, the maximum unambiguous range for this radar is about 100 km. In general, a higher PRF is designed for fire control radar as target information data for radar receiver processing is needed. The search radar has a lower PRF to satisfy a necessary longer detection range.

To avoid the problem of radar blind speed, the PRF of a radar can be changed within a range in a pseudo-random fashion. This modulation technique is known as "PRF jitter" and often has the additional benefit of making the radar more resistive to false target jamming. The range of this technique "jitters" rapidly about some mean value. The range of the jitter and the mean value are additional aids to signal recognition. An oscilloscope can be used to determine the width of the jitter excursion and a mean value of the PRF is estimated as lying within the center of this range. To find out the radar's PRF jitter range, one should measure the PRF first. As most radar has a maximum jitter value of 10% (AN/SPS-67), the jitter ratio is therefore 7.5% in the example where a radar's PRI = 1333 μs. To find out the jitter width, first, we use 7.5% multiple 1333 μs, the result of one site width is about 100 μs. However, the range of this "jitter" is around the mean or at a width of 200 μs. Figures 2.14 and 2.15 illustrate the PRF jitter condition.

Another modulation type commonly employed is that of the "PRF stagger". This method routinely switches the PRF back and forth between several values

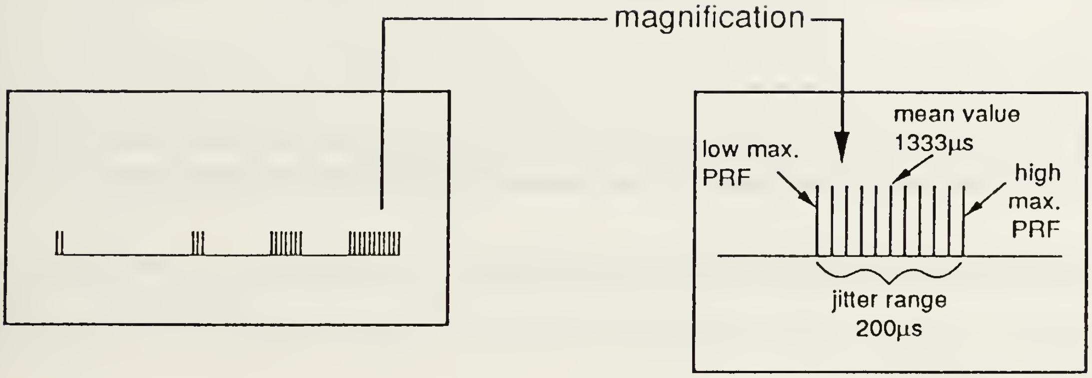

Figure 2.14: PRF Jitter View on Oscilloscope

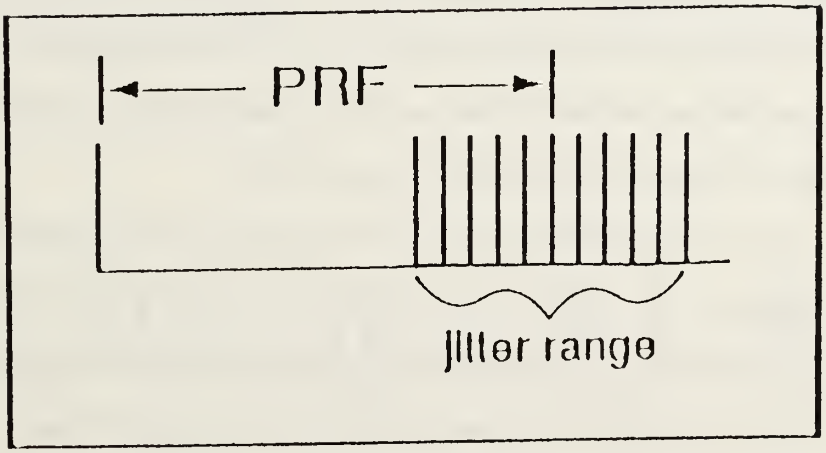

Figure 2.15: PRF Measurement on the Oscilloscope

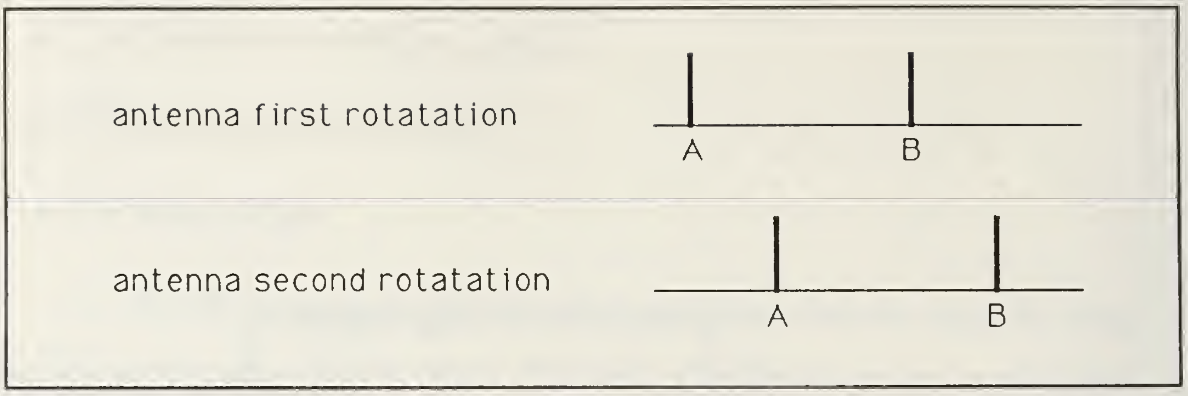

Figure 2.16: PRF Stagger Scan-to-Scan; antenna rotates twice, but both rotations cannot be seen at the same time on the oscilloscope

to eliminate problems of distance ambiguity and doppler speed. This type of modulation is usually used for air search radar and can be used by the EW operator for emitter identification.

The PRF can be switched on a pulse-to-pulse basis, or be kept on for a much longer period, roughly the time duration of one radar scan, labeled "scan-to-scan". Staggers are readily observable on the analysis oscilloscope and are yet another aid to recognition. The EW operator should understand that the scan-to-scan stagger PRF changes the PRF on an antenna rotation basis. It is impossible to observe the stagger PRF simultaneously on an analysis oscilloscope. The pulse-to-pulse stagger PRF is a different situation as it changes PRF on a PRI basis. Figures 2.16 through 2.19 show several kinds of stagger PRF.

The radar's PRF has a very important characteristic performance known as "PRF stability". The PRF stability of an intercepted radar signal is a key factor in helping the EW operator to identify the emitter platform. The actual stability of a radar's PRF is dependent upon the stability of its timing mechanism. This timing mechanism synchronizes the entire system and is usually a stable oscillating circuit or a crystal. Different radars are stable to differing degrees. These variances can be

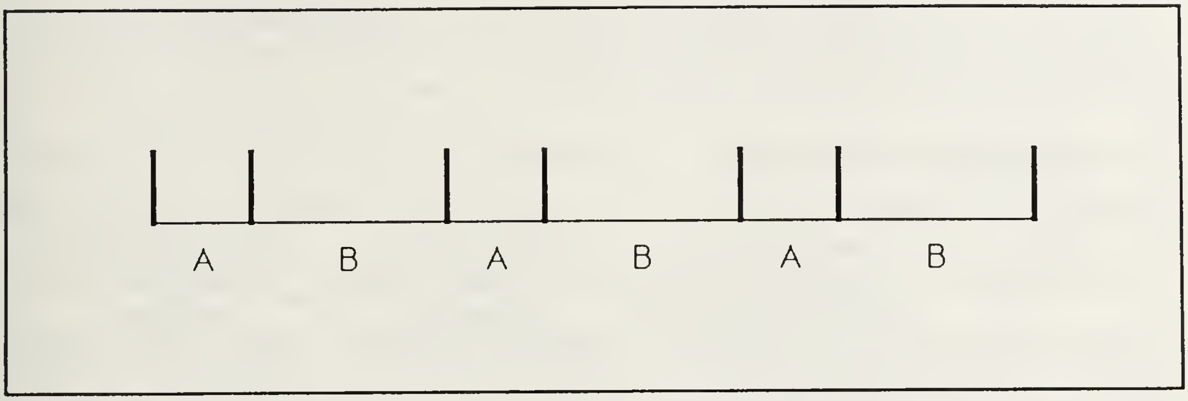

Figure 2.17: PRF Stagger "pulse-to-pulse" 2 element, 2 position

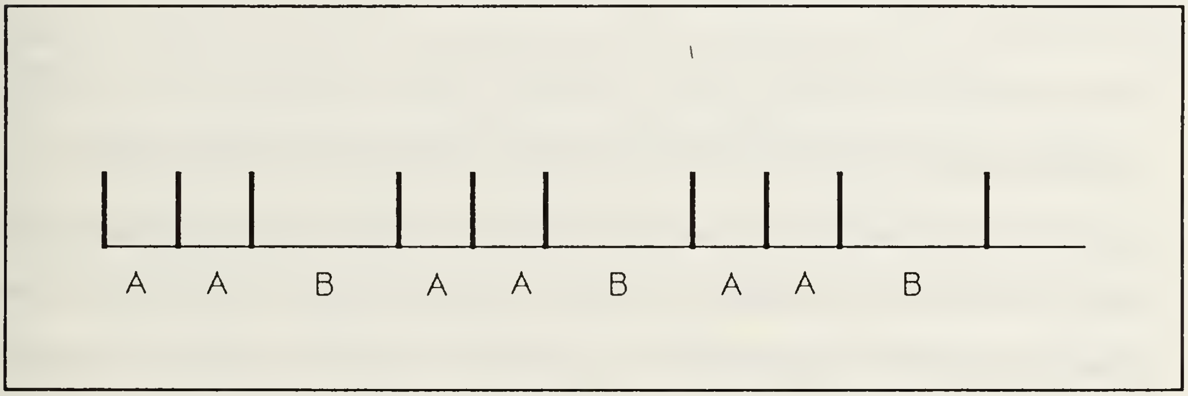

Figure 2.18: PRF Stagger "pulse-to-pulse" 2 element, 3 position

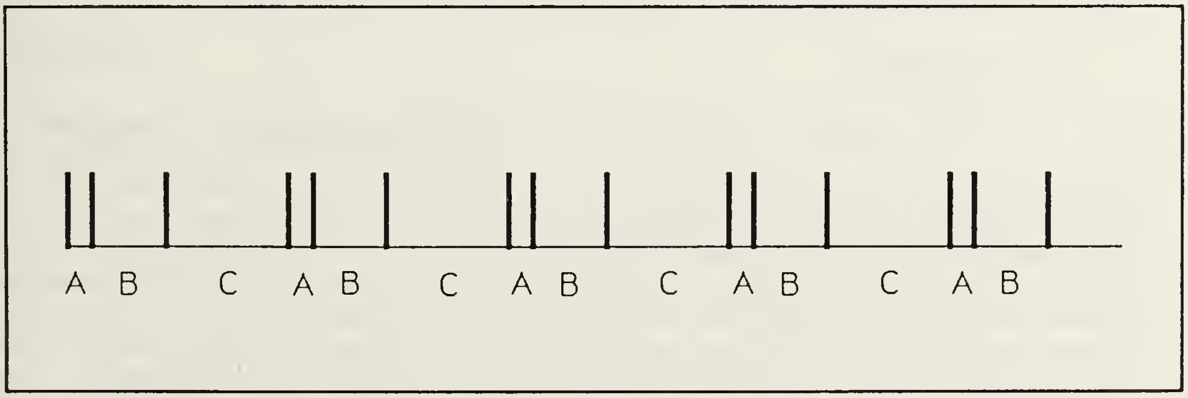

Figure 2.19: PRF Stagger "pulse-to-pulse" 3 element, 3 position

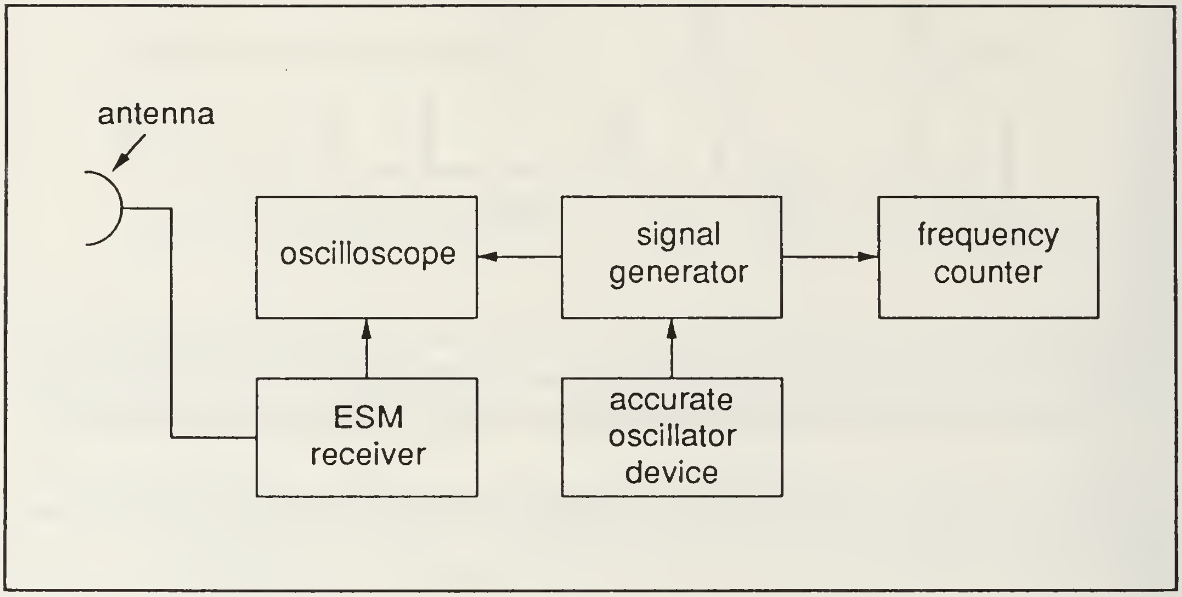

Figure 2.20: Fine PRF Measurement Using Standard Equipment

exploited for the discrimination or identification of radars. Accurate measurement requires a very stable time base in the ESM analysis equipment. Stability cannot be measured to a higher degree than that available by a particular system. The need for a temperature stable oscillator in the range of ± 0.0002 seconds is a requirement of a significant peacetime ELINT database. Figure 2.20 shows the whole system set up for measuring the fine PRF.

4. Scan Rate

Radar antenna scan rate is defined as the time required for one scan or cycle of the antenna to be completed. Since the radar pattern frequently shows amplitude variation, the measurment of the scan rate by automatic means can introduce ambiguity in finding the radar main beam; consequently, the intervention of an human operator may be required to resolve this detection ambiguity. The EW operator attenuates the receiving gain on the ESM receiver to make reception

of only the main lobe possible. The operator measures the complete cycle time when the antenna main lobe passes the ESM antenna. The time measurement is the scan rate. Scan rate is a valuable parameter to determine the radar's function. For example, a surveillance radar has a scan rate of about 15 RPM (4 seconds for one complete cycle). A multiple function radar scan rate can vary as the radar's function mode changes. The function mode can be changed to increase the number of pulses received by a radar, thus increasing the signal-to-noise ratio and improving the radar's detection capability.

Measurement of the scan rate is also dependent upon the type of the scan, posing a difficult problem for automatic systems. Circular scans are measured in seconds, or tens of seconds, whereas conical scans are measured in tens of Hz. The method of analysis requires first the identification of the scan type, then applying the appropriate measures to define the rate. Circular and sector scans may be measured with a stopwatch; however, complex fire control scans require an oscilloscope and a frequency counter for human operators. An automatic system must first be able to distinguish between the main lobe and the side lobes for scan determination. Based upon this information, the automatic system must be able to alter the process by which the periodic detection of energy is translated into a scan rate. This is not an easy problem.

C. SIGNAL RECOGNITION

The accuracy of radar recognition in automatic systems is a function of the accuracy of the input parameters and the completeness of the parameter library. The large number of radars used by military organizations and the civilian community have made the radar spectrum a crowded place. Often, parameters overlap in every area. In these cases, knowledge of geography, order of battle, or the tactical situation

must be used to determine the correct emitter type. Also, expert knowledge of signal types is important for accurate recognition.

There are conceivably many instances when a military organization could be forced to fight against systems with unknown parameters. The ability to determine a threat is only as good as the database. If an automatic system encounters a set of parameters that is unknown, the signal should be assigned to a human analyst to perform an analysis of "functional recognition". Functional recognition is defined when a radar's parameters do not fit a library entry. The next best option is to determine the "function" of the radar and to determine if the signal constitutes a threat.

Functional recognition is based on the premise that the physical operating parameters of the radar basically tell what the radar is used for. This is critical for enemy systems that pose a severe threat. For example, missile homing radars in the noses of surface-to-surface missiles all look "electronically similar". Without prior information, it may not be possible to identify the exact type of missile. However, for the tactical scenario at hand, a missile has been detected and appropriate countermeasures must be determined. The categories for such recognition are broad and not easily defined, leading to high false alarm rates. Nevertheless, false alarms are tolerated more easily than missile hits. Table 2.1 lists parameter ranges and their functional equivalents. Figure 2.21 indicates the procedure of target identification. Figure 2.22 illustrates the signal functional recognition and Figures 2.23 and 2.24 illustrate various types of radar signal functional recognition flowcharts.

TABLE 2.1: PARAMETER RANGES AND FUNCTIONAL EQUIVALENTS

EMITTER TYPE / PARAMETERS	FIRE CONTROL AND TRACKING RADAR	SHIPBOARD AIR-SEARCH RADAR	SHIPBOARD SURFACE SEARCH RADAR	LAND BASED AIR SEARCH RADAR	MISSILE
RF	8 -- 10 GHZ	200 -- 400 MHZ OR 1 -- 3 GHZ	8 -- 9 GHZ OR 5 -- 6 GHZ	100 -- 300 MHZ	8 -- 10 GHZ
PRF	1500 --2500 PPS	150 -- 300 PPS OR 2000 -- 2500 PPS	600 -- 800 PPS OR 1200 -- 1800 PPS	150 -- 400 MHZ	3000 -- 6000 PPS
PW	0.1 --0.5 US	5 -- 100 US	0.3 -- 1.0 US	4 -- 100 US	0.1 -- 0.25 US
SCAN TYPE	VERTICAL OR CONICAL	VERTICAL CIRCULAR	CIRCULAR	VERTICAL	sector UNISCAN COSRO
SCAN RATE	HARD TO MEASURE	4 -- 15 sec	4 -- 5 SEC	10 -- 16 sec	HARD TO MEASURE
MODULATION TYPE	JITTER PRF FIXED PRF	STAGGER FREQ. AGILITY FIXED PRF FMOP PMOP	JITTER PRF FIXED PRF	FREQ. AGILITY STAGGER FMOP PMOP FIXED PRF	STEADY

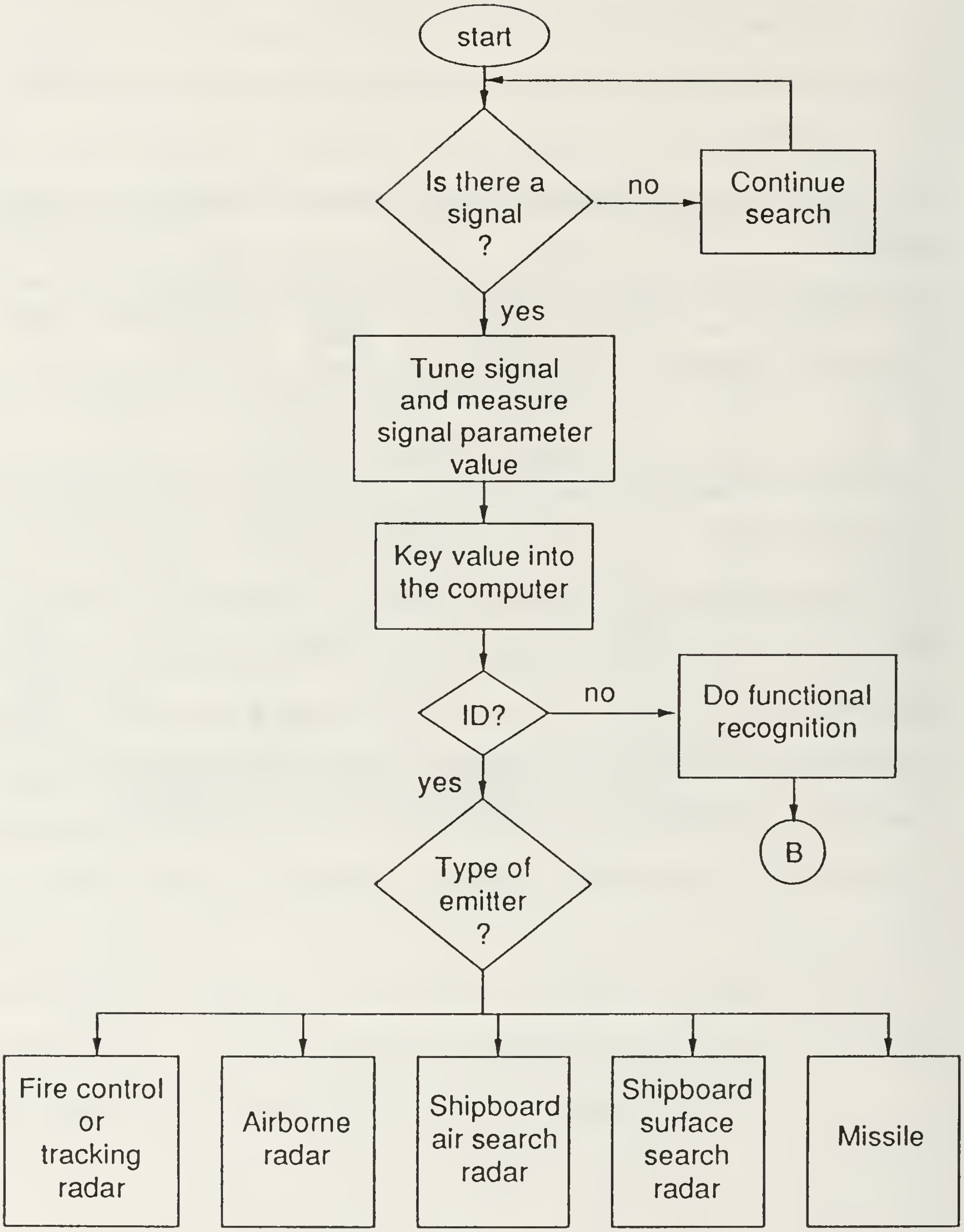

Figure 2.21: Target Identified Procedure

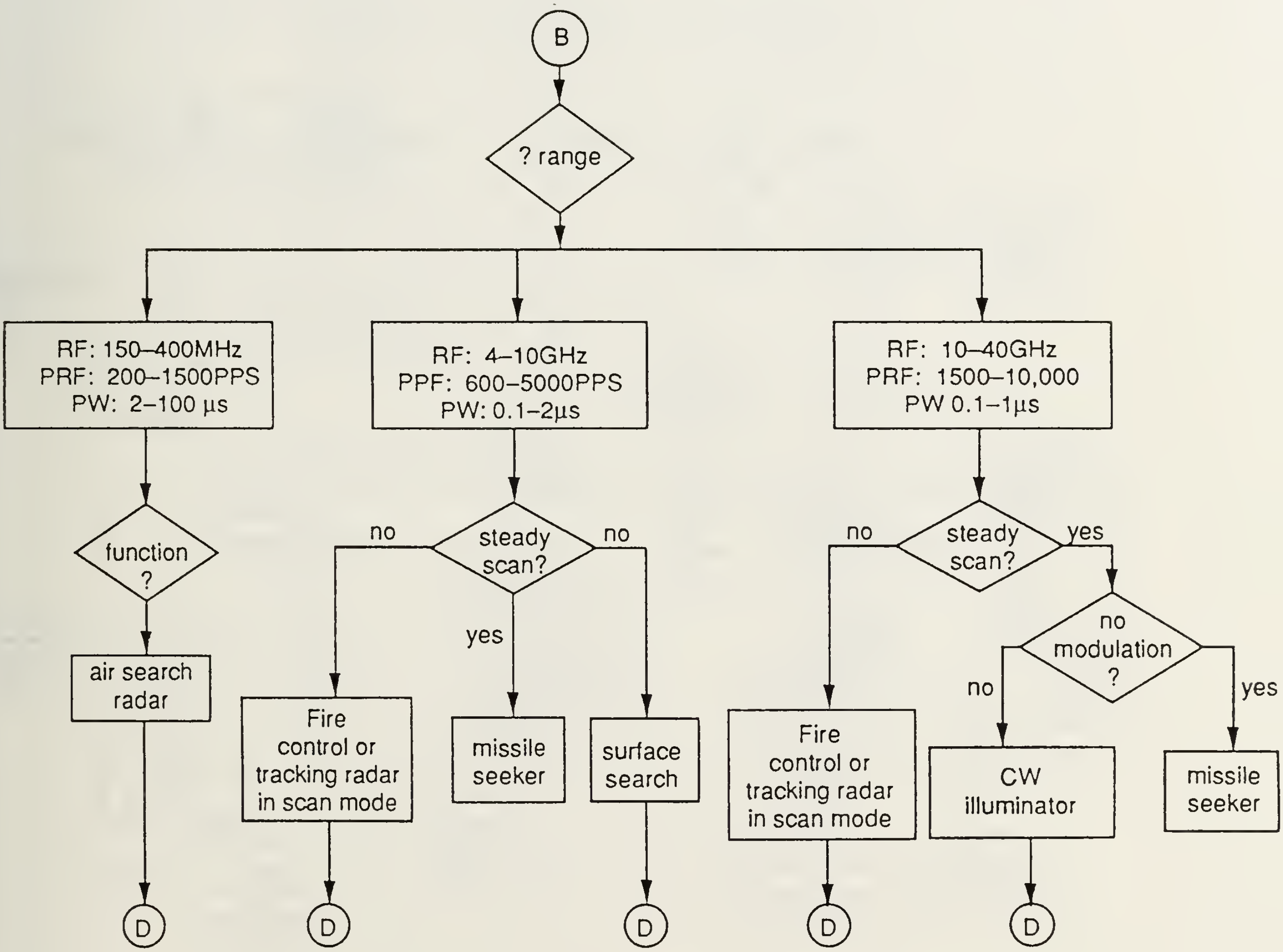

Figure 2.22: Functional Recognition for Several Types of Threat Signals

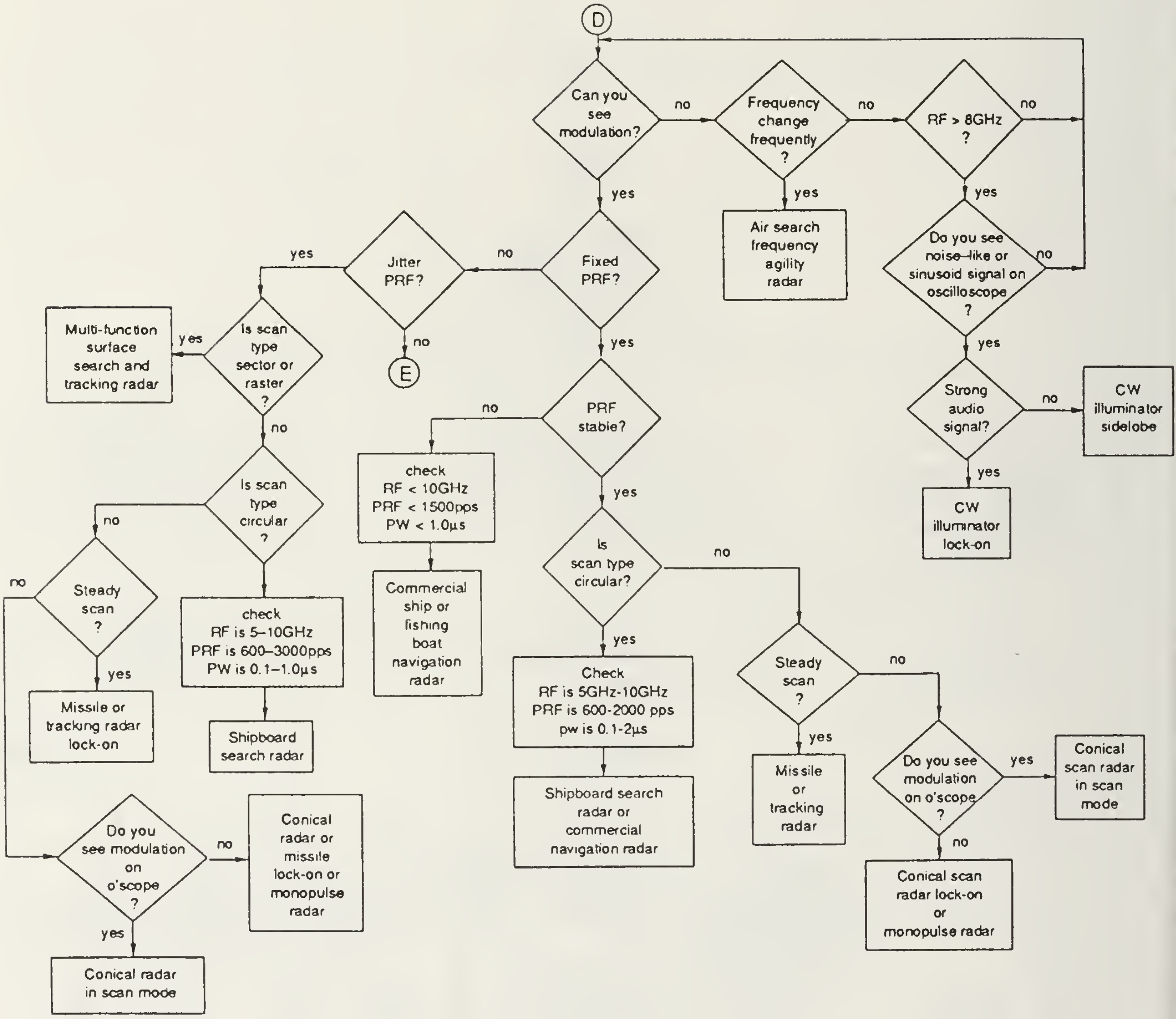

Figure 2.23: Functional Recognition for Several Types of Radar

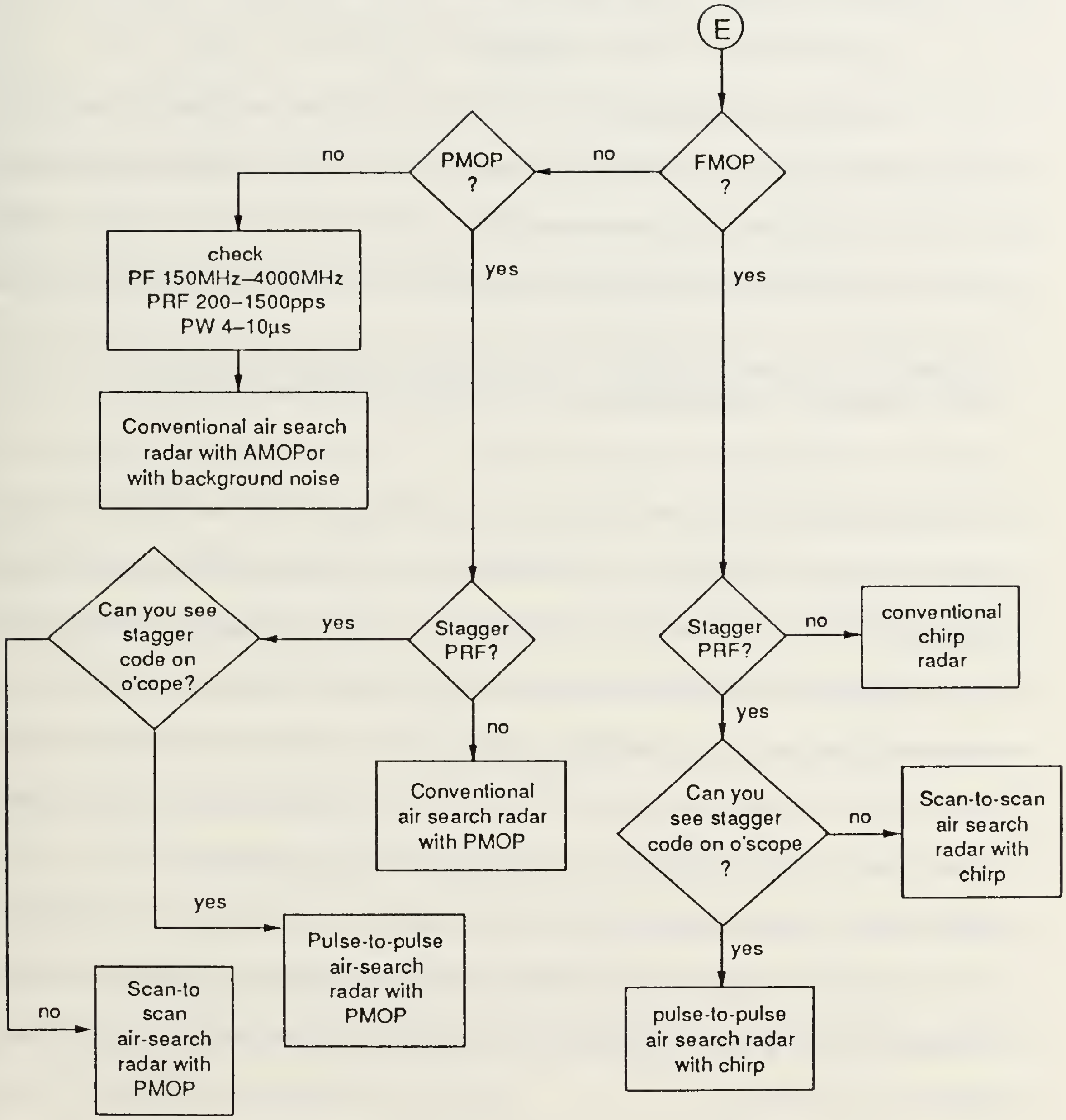

Figure 2.24: Functional Recognition for Several Types of Radar

III. EXPERT SYSTEM CONCEPTS

A. Artificial Intelligence (AI) and Expert System

1. AI Definitions and Concepts

Artificial intelligence (AI) is a branch of computer science, the art of making systems for the intelligence community. The field of artificial intelligence offers solutions for complex problem solving. Patrick H. Winston, director of the artificial intelligence laboratory at the Massachusetts Institute of Technology, writes:

> The goals of artificial intelligence are to make computers more useful and to understand the principles which make intelligence possible. [Ref. 8]

AI is concerned with the programming of computers to perform tasks that are presently manually performed. AI technology can therefore lead to a number of useful applications. The design of AI research is to create computer programs that capture the knowledge and reasoning processes of highly intelligent specialists. In recent years, there has been an explosive growth in the number of military AI systems oriented toward providing operational status, advice and information to the military decision makers. One of the best examples of military applications related to EW is the Large Area Surveillance Sensor System (AELASS) [Ref. 9]. The AELASS system is oriented toward providing better use of surveillance mode data including the detection of targets, the maintenance of an activity level history, and estimates of enemy activity levels.

The AELASS system operates via the rule-base component which contains the knowledge utilized for the system analysis of indicators and activities. [Ref. 9] The rule base is composed of expert knowledge in the form of rules. A rule is a

collection of conditions and the actions to be taken if the conditions are met. In this thesis, a rule-based program is developed to perform threat identification and is discussed in Chapter IV.

2. Expert System Definition and Concept

a. What is an Expert System?

An expert system is a computer program that possesses knowledge on a specialized subject and solves problems or gives advice about that subject. [Ref. 10] The expert system field provides methods and techniques to aid users in solving real-world problems. They are also called knowledge-based systems because they require domain-specific knowledge necessary for solving problems. A knowledge-based system applies rules of thumb to a symbolic representation of knowledge, rather than employing algorithmic method. This knowledge is obtained by a knowledge engineer who gathers knowledge from domain-specific experts about a particular subject. The knowledge, then, is used to develop the knowledge base for use in an expert system. A knowledge base in the abstract sense consists of descriptions and procedures, expressed as facts and rules, in an expert domain. A knowledge based system is commonly referred to as a rule-based system since most problem solving strategies are encoded as rules.

Information about the problem to be solved can be incomplete or unreliable and relations is the problem domain can be approximate. For example, we may not be able to measure the same emitter signal simultaneous from various types of ESM with the same result, or know that the measurement data is absolutely correct. This requires probability reasoning.

b. Basic Structure of an Expert System

Three basic elements of an expert system are: a knowledge base, an inference engine, and a user interface. The knowledge base contains domain-specific knowledge, represented by rules that specify the action to be carried out when prerequisite conditions are satisfied. The rules are acquired from human experts and are normally expressed as condition-action pairs similar to an IF-THEN statement:

IF certain conditions are true

THEN perform the following actions

The inference engine uses information presented in the rule base to infer conclusions and to control overall execution. It can be regarded as a rule interpreter. The reference engine consists of procedures that determine the correct application of the rules. It also controls the order of rule activation and rule selection when more than one rule are applicable. A user interface provides a mechanism for information interchange between the user and the expert system. The interface and the inference engine may be viewed as one module, called a shell or an expert system shell. Figure 3.1 illustrates the basic expert system architecture.

B. EXPERT SYSTEM CONSTRUCTION

The main elements which relate to the expert system are the human expert, the development tool, the knowledge engineer, and the user. Figure 3.2 illustrates the expert system process and each of the basic element functions.

A knowledge engineer is the person who acquires the knowledge from the domain expert and transports it to the knowledge base. The domain expert is a knowledgeable person who tells the knowledge engineer what rules to add or modify. The knowledge engineer discusses these with the domain expert and makes appropriate changes to the knowledge base.

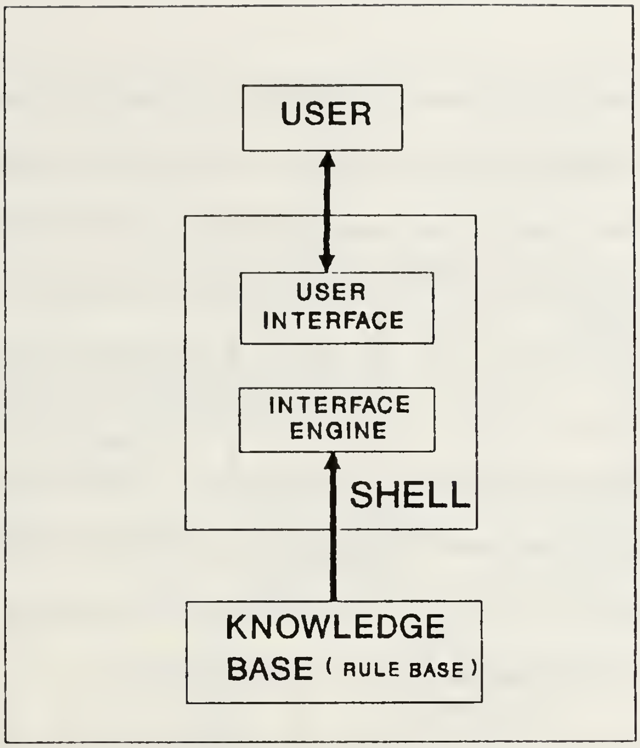

Figure 3.1: Basic Architecture of an Expert System

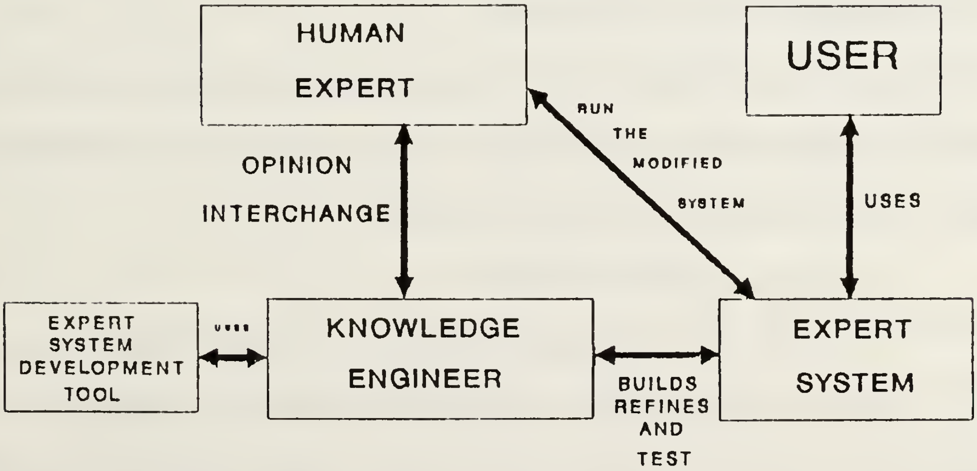

Figure 3.2: An Expert System Process

An expert system development tool is the programming language tied in with associated support facilities and is utilized by the knowledge engineer to build an expert system. These tools differ from procedural programming languages such as Pascal, Ada, FORTRAN, or C. In this thesis, a knowledge base is developed in CLIPS, and expert system shell written in C [Ref. 11]. Facts are essential to complete an execution in CLIPS. A fact consists of one or more fields enclosed in matching left and right parentheses. For example, (Steady Scan) has two fields while (Steady-Scan) has only one field. The basic elements of CLIPS are the fact-list, the global memory for data, the knowledge-base containing all the rules, and the inference engine which controls the overall execution.

The user is the human who applies the system's expertise in solving a specific task. For the purpose of this thesis, the user is the EW operator or anyone who needs to use the system. Figure 3.2 demonstrates the user operation of the system to reach an answer, the knowledge engineer refining the existing knowledge in the system, and a domain expert adding new knowledge and running the modified system.

C. A Rule-Based System for EW

This section provides our view in applying expert system technology to EW. It should be emphasized that the purpose is to provide a tool to aid, instead of to replace, the EW operators in decision-making.

1. A Typical Scenario at Sea

This thesis attempts to develop a "rule-based" expert system prototype for target identification and decision making for counter measure in the area of electronic warfare. It is aimed at improving the target identification capability of systems currently used aboard naval ships. A basic structure of an expert system as applied to improving an EW system is shown in Figure 3.3. Figure 3.3 shows

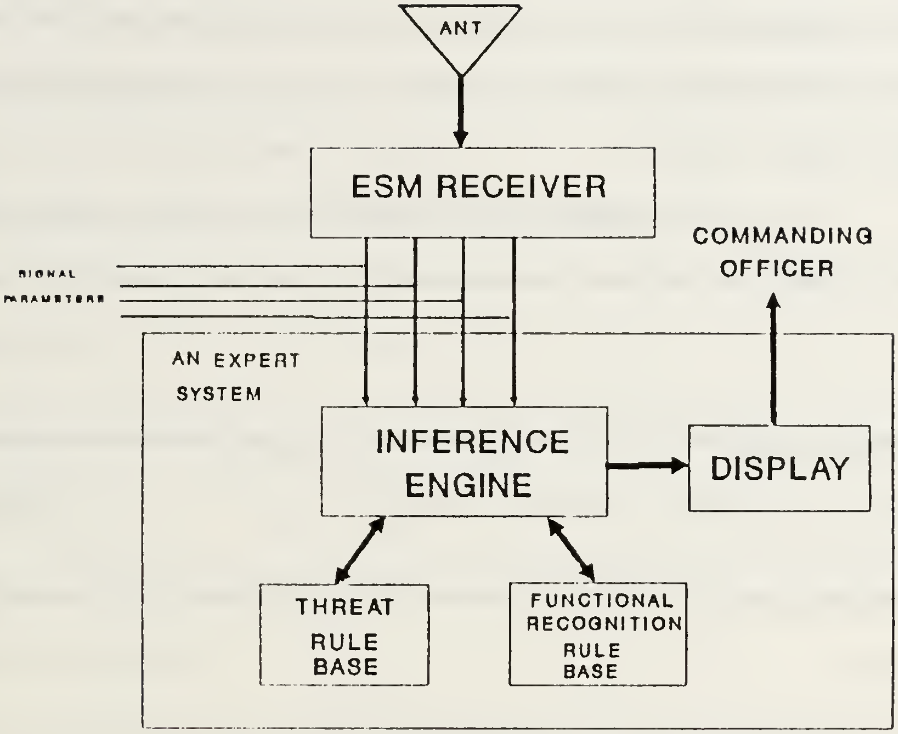

Figure 3.3: The Structure of a Ship's EW Rule Based System

that the use of an expert system aids the ESM system in performing target identification. The signals of interest are intercepted by the ESM receiver and tuned to obtain the basic signal parameters, which include the RF, PRF, PW, and scan rate. The expert system receives the basic parameters from the ESM receiver and allows these input parameters to give the best correlation in a programmable rule-based system. When correlation processing is complete, the expert system displays the information for decision making to the Commanding Officer.

Most fleet ships in the current navies employ the ESM system to perform the warning and identification mission. ESM systems installed on ships rely on the ship's design purpose and the mission characteristics. Automatic ESM

systems are employed if ships are conducting operational missions. However, manually operated ESM systems tend to be used in the ship's non-operational missions, for example, logistic support.

An automatic ESM system performing automatic target identification does not require a rule based system unless the following conditions are applicable:

- The threat library database is limited to only signal parameters collected from ELINT or if the library contains insufficient data.
- If the reserve mode of a certain emitter has been changed by the enemy during combat.

The scenario considered here is that of a naval ship performing a patrol mission in a specific area. Ships equipped with nonautomated ESM systems must perform manual target identification. The object of the ESM mission is to obtain and process the intercepted signals accurately. Although the ship's EW system is staffed by competent and experienced operators, their vigilance, enthusiasm, and effectiveness may be severely reduced in a dense electronic environment when using manual equipment. This could be a result of fatigue caused by a ship's long patrol or other operational constraints. As the EW view is tasked to evaluate and report intercepted signals to the combat information center officer (CICO), the EW operator may sometimes make incorrect evaluations, as a result of the factors described above. Tactical decisions made by the ship's commanding officer rely heavily upon the resultant target identified by the EW operator. Although automatic ESM systems are employed on ships, target identification and evaluation is still completed via a human operator unless the threat library is sufficiently informed and accurate.

Thus, the EW operators play an indispensable role in the commanding officer's decision making process. Any mistake made by the EW operators can precipitate potentially unsafe consequences to the ship.

2. Advantages of an EW Rule-Based System

The following are the advantages that might be gained with the EW rule-based system:

- A decrease in the average processing time needed to identify a threat by EW operator
- A decrease in the probability of human errors in the complex and dense electronic environment
- Can be used as an EW subsystem to generate a functional recognition method to overcome the unknown situation.

3. Main Structure of EW Rule-Based System

We have discussed the purpose of an expert system and the importance of using a rule-based system. The EW rule-based system is used as an EW subsystem. The system receives preprocessed ESM receiver inputs, determines what radar signals are present, performs threat target identification, and suggests the best possible electronic counter measure. If the system does not correlate with the input signal parameters, an "unknown" situation occurs. Unknown problems can be solved with the use of the system's functional recognition.

According to the above system's capability description, a design of the ship's EW rule-based system structure is shown in Figure 3.3. This system consists of the following units:

a. Inference Engine

The primary role of the inference engine is the control and use of the knowledge presented in the rule base and input data.

b. Rule Base

The rule base contains knowledge information data written in rule form for inferencing, allocating, and consulting procedures.

c. Display

The display unit provides output information to the decision level and allows the EW operator to input information. This information exchange is completed by using a keyboard, a terminal, and a mouse.

IV. AN EXPERT SYSTEM FOR EW

A. PROGRAM STRUCTURE

This electronic warfare rule-based system is written in CLIPS, an expert system shell created by Artificial Intelligence Section (AIS) at NASA/Johnson Space Center (JSC). CLIPS specifically provides high portability, low cost, and easy integration with external systems. The primary method of representing expert knowledge within CLIPS is in the form of rules. The rules, as discussed in Chapter III, are acquired from the domain-expert and are normally in the form of CONDITION-ACTION pairs such as:

IF the measured signal is steady scan (condition)

THEN the source may be a missile (action)

Figure 4.1 shows an example of some EW rules. The rules are designed and stored in the knowledge base according to the threat parameters for a specific generic area. The system program contains two parts, the threat parameter database and the functional recognition database (See Appendix A). The system program operates in a forward-chaining mode, a type of data driven control strategy in which rules are applied to the fact or object attributes for the formulation of an hypothesis.

B. SYSTEM CHARACTERISTICS

The computer used for the rule-based system prototype program is an IBM-PC compatible minicomputer system running MS-DOS 4.01 operating system. The computer system requires 3.75M bytes hard disk and 640K bytes of RAM to run the EW rule-base program.

```
(defrule input -1
⇒ (printout t crlf ''Can you see modulation?''  crlf)
(assert (modulation = (read)))
(defrule mod (modulation no)
⇒ (printout t ''FREQ larger than 10 GHZ?'' crlf )
(assert (FREQ = (read)))
(defrule case (FREQ yes)
⇒ (printout t ''noise like or sinusoid signal on the oscilloscope?''  crlf)
(assert (Noiselike-Sinusoid Signal yes)
(defrule NLSS (Noiselike-Sinusoid Signal yes)
⇒ (printout t crlf ''strong signal audio?''  crlf)
(assert (strong-audio = (read)))
(defrule strong-audio (strong-audio yes)
⇒ (printout t ''CW illuminator lock ON'' crlf))
```

Figure 4.1: An Example of EW Rule Base for CW Illuminator Status

A notable characteristic designed for this system is that the rule base program can be improved at the EW expert knowledge level rather than at the level of the design program. Thus, modifications may be made directly to the expert knowledge domain in the rule-base, rather than modifying the structure of the program.

Another characteristic of the system is that the rule-based system program operates by logical reasoning rather than by calculation, such as that used in other types of programs. An important component of the rule-base is the number of facts, representing related information, stored in fact-lists in the computer memory. Rules are executed based on the existence or non-existence of these facts.

C. SYSTEM OPERATION

The EW rule-based system operates by a data driven control strategy. This approach is started when the EW operator inputs information into the rule-based system. The inference engine then selects a knowledge source and scans for any

rules that can be fired, applies these rules towards generating a conclusion, and then waits for further input until a final goal is reached.

When the rule is compiled to start the system, the user is presented with menus to initiate the program. The user will be asked for input. The EW operator then keys the known basic signal parameters into the expert system for target identification. If an unknown situation occurs, the program allows the EW operator to perform functional recognition. To support the EWO decision making effort, the rule base contains some ECM techniques that can be suggested to allow a correct ECM decision.

D. SYSTEM LIMITATIONS

Absolutely perfect target identification systems do not exist in the EW world. Using an automatic ESM system allows for operation in a dense radar environment with the ability to perform threat identification. To meet the requirements, the ESM system must provide the capability to overcome a complex signal of a radar scan pattern. However, an automatic ESM system has some process limitations when dealing with such a radar signal. For example, both monopulse or conscan radars exhibit a steady scan signal, which is difficult to measure with a computer-based ESM system. This is also true if an intercepted signal exhibits a missile lock onto the ESM site. However, this problem may be solved when the programmable library of emitter data contains sufficient knowledge. The following questions will be addressed in this case: How is the intelligence source guaranteed to provide such complete information to the ESM system? What indication is there that the enemy will not use the reserve mode during combat? These questions must be answered via a functional recognition method.

Ships using non-automatic ESM systems have their own limitations. In Chapter III, we discussed a generic scenario for a ship at sea. We understand that the ESM system operates manually, and that effectiveness is affected by various environment factors. In this thesis, a prototype program was developed to determine the feasibility and suitability of a rule-based system that could improve the threat identification capability of non-automatic ESM systems currently used aboard naval ships. The prototype was evaluated to determine the potential of its use as an EW subsystem by running a simulation program. In general, the prototype EW rule-base system was found to have the limitations described below:

1. System Response Time

The current EW rule-based system requires manual input and therefore, the time required for target identification relies on the human input response time.

2. Threat Library Parameters Overlapping

Any ESM system faces an increasingly complex signal environment. The EW rule-based system effectiveness decreases due to signal ambiguities in the threat environment.

3. Unknown Situation

The system program uses four signal parameters to perform threat identification, one of which is the scan rate. The scan rate is difficult to measure when the intercepted signal has the property of a complex scan. Threat identification cannot be accomplished if scan rate information is not available or if the intelligence source is weak.

E. PROGRAM SIMULATION

This section provides simulation reults to examine how closely the system's performance meets the design objectives. Test runs performed for various threat signal situations are listed below.

1. Case 1: Surface Search/Missile-Targeting Radar Operating in Multi-function Mode and Suggested ESM Technique

Frequency in MHZ?
/: *8600*
PRF in PPS?
/: *1200*
PW in μs?
/: *0.32*
Scan-rate in sec?
/: *4.0*

"This is Square Tie Radar in Navigation Mode"
"ECM Choice FM-by Noise and Chaff"

Frequency in MHz?
/: *9100*
PRF in PPS?
/: *2500*
PW in μs?
/: *0.25*
Scan-rate in sec?
/: *2.0*

"Square Tie in Combat Mode!!"
"Fire Chaff!!"
"IF no/low modulation fire IR flare"
"ECM choice countdown + swept audio + noise"
Reset system

Note: "/:" is the system prompt and the user input is shown in italic.

This scenario depicts the situation in which the threat emitter can be used for operation in the multimode function, i.e., navigation mode and combat mode.

The radar is designed to provide the necessary information to the missile system. There are some different signal parameter ranges between the navigation mode and combat mode due to the radar's operational function. In combat mode, the radar signal parameter has been changed within certain ranges when it is compared to the radar navigation mode. This change does not affect the type of radar to be used. The system can distinguish this situation and will suggest the best electronic counter measure to be taken.

2. Case 2: A Various Type of Emitter Functional Recognition

Can you see modulation?
/: *n*
Frequency change frequently?
/: *n*
RF > 8GHz?
/: *y*
Noise-like or sinusoid signal on oscilloscope?
/: *y*
Strong audio signal?
/: *n*
CW illuminator sidelobe

Strong audio signal appear?
/: *y*
CW illuminator lock-on
Reset system - - - -
Fixed PRF?
/: *y*
PRF stable?
/: *y*
Is scan type circular?
/: *yes*
RF is 5 GHz, PRF is 600-2000 pps, PW is 0.1 in 2 μs?
/: *y*
Shipboard search radar or commercial navigation radar

Is steady scan?
/: *y*
Missile or tracking radar
Steady scan disappear?
/: *y*
Modulation?
/: *y*
Conical scan radar in scan mode
Modulation?
/: *n*
Conical scan radar lock-on or monopulse radar
Reset system - - - -

Note: "/:" is the system prompt and the user input is shown in italic.

In this case, the ship's ESM system intercepts the signal, and since the rule-base library was insufficient, an unknown situation occurred. The use of functional recognition is required for identification of the signal emitter.

V. CONCLUSIONS

A. SUMMARY

This thesis emphasizes using an expert system approach for the design of an electronic warfare threat identification system. This method can improve the ship's nonautomatic ESM system and assist the electronic warfare operator in performing target identification. The system can also assist the Electronic Warfare Officer in making the best ECM decision in a threat signal environment.

Chapter I outlined the objectives and problems of building such a system. Chapter II presented the basics of the Electronic Warfare domain knowledge. Chapter III enumerated basic concepts of expert system structures and presented a real encounter situation when non-automatic ESM systems are used. Chapter IV presented our prototype implementation and demonstrated its use through several simulation runs.

B. FUTURE WORK

The simulation results in the previous chapter have sufficiently demonstrated the feasibility of using a knowledge based expert system in the EW domain. To provide real time information to the EW operator, or EW officer, the system needs to be fully integrated into the ship's ESM and weapon systems. Future efforts should address the possibility for expert systems to maintain the present situation at all times, rather than to wait for manual inputs. The goal of a fully integrated EW rule-based system will be a complicated task, but is essential for the future success in the Electronic Warfare world.

APPENDIX A

Rule-Base Program

```
; This is a rule base of EW for functional
; recognition, file created by LCDR
: WEN CHENG HSIUNG R.O.C Navy

 (defrule case-1
  =>
 (printout t " Can you see modulation ? " crlf)
 (assert ( modulation =(read))))
  (defrule case-2   (modulation no)

  =>
  (printout t " Frequency larger than 10 GHZ ? "
   crlf)
  (assert (FREQ =(read))))

  (defrule case-3
  (FREQ yes)
  =>
  (printout t " noise like or sinusoid signal on
   the oscilloscope ? " crlf)
  (assert (NoiseLike-SinusoidSignal =(read))))

  (defrule NoiseLike-SinusoidSignal
  (NoiseLike-SinusoidSignal yes)

  =>
   (printout t " Strong signal audio ?  " crlf)
   (assert (Strong-audio =(read))))

   (defrule Strong-audio
   (Strong-audio yes)
   =>
   (printout t " CW illuminator lock-on " crlf ))

   (defrule ret
   ( FREQ no)
   =>
   (printout t " Go back to start (reset system)
    " crlf))
   (defrule case-4
   (Strong-audio no)
   =>
   (printout t " CW illuminator sidelobe" crlf))
```

```
(defrule case-5
(NoiseLike-SinusoidSignal no)
=>
(printout t " Go back check modulation" crlf))
(defrule case-7
(modulation yes)
=>
(printout t " FIXED-PRF ?  " crlf)
(assert (FIXED-PRF =(read))))

(defrule FIXED-PRF
(FIXED-PRF yes)
=>
(printout t " PRF stable ?  "  crlf)
(assert (PRF-stable =(read))))

(defrule PRF-stable
(PRF-stable yes)
=>
(printout t " Is scan type circular ?  " crlf)
(assert (Scan-Type =(read))))

(defrule Scan-Type
(Scan-Type yes)
=>
(printout t " Check IF RF range is 5 GHZ to
                            10GHZ
                        PRF range is 600 to 3000
                        PW  range is 0.1 to 2.0 US
 then this signal is Shipborne search radar or
          commercial navigation radar " crlf))


 (defrule case-8
 (Scan-Type no)
 =>
 (printout t " Is steady scan ?  " crlf)
 (assert (steady-scan =(read))))

 (defrule steady-scan
 (steady-scan yes)
 =>
 (printout t " This signal is Fire Control Radar
             or Tracking Radar Lock-on " crlf))
```

```
(defrule case-9
(steady-scan no)
=>
(printout t " modulation on oscilloscope ? "
 <yes> or <no> "crlf)
(assert (modulation-on-Oscilloscope =(read))))
(defrule modulation-on-Oscilloscope
(modulation-on-Oscilloscope no)
=>
(printout t " This is Fire Control Radar or
  Tracking Radar lock-on "
   crlf))
 (defrule scan
(modulation-on-Oscilloscope yes)
=>
(printout t " This signal could be conical scan
 radar or monopulse, lobe radar " crlf))
(defrule case-1-0
(PRF-stable no)
=>
(printout t "  RF  < 10GHZ ?
               PRF < 1500 PPS ?
               PW  < 1.0 ?

               If   true

               then  this is commerical ship

               else fishing boat Radar with
               oscilloscope unstable " crlf))

(defrule case-1-1
(FIXED-PRF no)
=>
(printout t " JITTER PRF ?  " crlf)
(assert (JITTER-PRF =(read))))
(defrule JITTER-PRF
(JITTER-PRF yes)
=>
(printout t " Is sector scan(or raster scan)?
 "crlf)
(assert (sector-raster =(read))))
(defrule sector-raster
(sector-raster yes)
=>
```

```
(printout t " This is Multi-function surface
              search radar
              or Tracking radar " crlf))
(defrule called
(sector-raster no)
=>
(printout t  crlf "  Is circular sacn ?
 "crlf)
(assert ( circular =(read))))
(defrule circular
(circular yes)
=>
(printout t crlf " Check the RF 5000 MHZ to
                   10 GHZ
                   PRF 600 to 3000
                   PW  0.1 to 1.0 US

                    IF  true

      then  Shipborne search radar " crlf))

(defrule input
(circular no)
=>
(printout t " Is steady scan ?  " crlf)
(assert (steady =(read))))
(defrule steady
(steady yes)
 =>
 (printout t " If strong audio then this
  signal could be Tracking radara
  (fire control radar) or A
       Missile " crlf))

(defrule input-1
(steady no)
=>
(printout t " Check RF is 5000 MHZ to 10GHZ
                    PRF is 600 to 3000 PPS
                    PW  is 0.1 to 1.0 US
              IF  true
 then  this signal is shipborne search radar
 "crlf))
 (defrule jitter(JITTER-PRF no)
  =>
```

```
(printout t "Check frequency counter readout
 if PRF stable
            Then  this is not jitter radar

    go back to start (reset system) " crlf))
```

This is a rule base of EW for threat identification file created by LCDR Wen Cheng Hsiung R.O.C Navy

```
(defrule signal-1
(freq ?x&:(>= ?x 8600))
(freq ?x&:(<= ?x 8800))
(prf ?input&:(>= ?input 1150))
(prf ?input&:(<= ?input 1250))
(pw  ?pulse&:(>= ?pulse 0.25))
(pw  ?pulse&:(<= ?pulse 1.0))
(scan_rate ?call&:(>= ?call 3.6))
(scan_rate ?call&:(<= ?call 4.2))
=>

(printout t "This is Square Tie radar in navigation
mode" crlf)
(printout t "ECM choice FM-by-noise and chaff " crlf))

(defrule signal-2
(freq ?x&:(>= ?x 9000))
(freq ?X&:(<= ?x 9200))
(prf ?input&:(>= ?input 2000))
(prf ?input&:(<= ?input 2500))
(pw  ?pulse&:(>= ?pulse 0.25))
(pw  ?pulse&:(<= ?pulse 1.0))
(scan_rate ?call&:(>= ?call 2))
(scan_rate ?call&:(<= ?call 3))
=>

(printout t " This is Square Tie radar in Combat mode
!! " crlf)
(printout t " fire chaff !!!" crlf)
(printout t " If no/low modulation fire IR flare
 and
 ECM choice countdown+swept-audio+noise!!! " crlf))

(defrule signal-3
(freq ?x&:(>= ?x 9250))
(freq ?x&:(<= ?x 9500))
(prf  ?input&:(>= ?input 2000))
(prf  ?input&:(<= ?input 2500))
(pw  ?pulse&:(>= ?pulse 0.25))
(pw  ?pulse&:(<= ?pulse 1.0))
(scan_rate ?call&:(>= ?call 2))
(scan_rate ?call&:(<= ?call 3))
```

```
(printout t " This is Square Tie radar in Combat
 mode !! " crlf)
(printout t " fire chaff !!!" crlf)

(printout t " If no/low modulation fire IR flare
 ECM choic countdown+swept-audio+noise!!!" crlf))


 (defrule signal-4
 (freq ?x&:(>= ?x 9500))
 (freq ?x&:(<= ?x 10000))
 (prf ?input&:(>= ?input 1500))
 (prf ?input&:(<= ?input 5000))
 (or
 ?fact <- (pw 0.5)
 ?fact <- (pw 10.0)
 ?fact <- (pw ?pulse&:(&&(>= ?pulse 2)(<= ?pulse 4
 ))))
 (scan_rate ?call&:(>= ?call 2.5))
 (scan_rate ?call&:(<= ?call 4))
 =>
 (retract ?fact)
 (printout t " This is B-class Fire Control radar
 "crlf))
 (defrule signal-5
 (freq ?x&:(>= ?x 9350))
 (freq ?X&:(<= ?x 9500))
 (prf  ?input&:(>= ?input 999))
 (prf  ?input&:(<= ?input 1100))
 (pw   ?pulse&:(>= ?pulse 0.1))
 (pw   ?pulse&:(<= ?pulse 0.3))
 (scan_rate ?call&:(>= ?call 3))
 (scan_rate ?call&:(<= ?call 4))
 =>

 (printout t "this is C-class navigation radar"crlf))

 (defrule signal-6
  (freq ?x&:(>= ?x 9200))
 (freq ?x&:(<= ?x 9400))
 (prf  ?input&:(>= ?input 3500))
 (prf  ?Input&:(<= ?input 4000))
 (pw   ?pulse&:(>= ?pulse 0.2))
 (pw   ?pulse&:(<= ?pulse 0.4))
 (scan_rate ?call&:(>= ?call 3))
 (scan_rate ?call&:(<= ?call 4))
```

```
=>

(printout t " This is D-class Fire control radar"
crlf))
(defrule signal-7
(freq ?x&:(>= ?x 8500))
(freq ?x&:(<= ?x 8600))
(prf  ?input&:(>= ?input 1200))
(prf  ?input&:(<= ?input 1300))
(pw   ?pulse&:(>= ?pulse 0.3))
(pw   ?pulse&:(<= ?pulse 0.5))
(scan_rate ?call&:(= ?call 2.5))
=>

 (printout t " This is E-class ss radar in
  search mode" crlf))

(defrule signal-8
(freq ?x&:(>= ?x 8500))
(freq ?x&:(<= ?x 8600))
(prf ?input&:(>= ?input 1000))
(prf ?input&:(<= ?input 1050))
(pw  ?pulse&:(>= ?pulse 0.5))
(pw  ?pulse&:(<= ?pulse 0.8))
( or
 (scan_rate 4.0))
=>

(printout t "This is an E-class surface search
 radar in navigation mode " crlf))

(defrule signal-9
(freq ?x&:(>= ?x 8500))
(freq ?x&:(<= ?x 8600))
(prf ?input&:(>= ?input 3000))
(prf ?input&:(<= ?input 3150))
(pw  ?pulse&:(>= ?pulse 0.2))
(pw  ?pulse&:(<= ?pulse 0.4))
(or
(scan_rate 4.0))

=>
(printout t "This is an E-class surface search
 radar in combat mode " crlf)
 (printout t"Fire chaff and IR flare ! crlf"))
```

```
(defrule signal-1-0
(freq ?x&:(>= ?x 200))
(freq ?x&:(<= ?x 210))
(prf ?input&:(>= ?input 250))
(prf ?input&:(<= ?input 400))
(pw  ?pulse&:(>= ?pulse 2.0))
(pw  ?pulse&:(<= ?pulse 5.0))
(scan_rate ?call&:(>= ?call 12.0))
(scan_rate ?call&:(<= ?call 15.0))
=>

(printout t "This is  ?Type air search radar
 "crlf))
(defrule signal-1-1
(freq ?x&:(>= ?x 5000))
(freq ?x&:(<= ?x 5050))
(prf ?input&:(>= ?input 640))
(prf ?input&:(<= ?input 650))
(pw  ?pulse&:(>= ?pulse 0.4))
(pw  ?pulse&:(<= ?pulse 0.5))
(scan_rate ?call&:(>=
  ?call 3.6))
(scan_rate ?call&:(<= ?call 4.2))
=>

(printout t "This is  G-class surface search
 "crlf))
(defrule signal-1-2
(freq ?x&:(>= ?x 1000))
(freq ?x&:(<= ?x 1030))
(or
 (prf  3048)
 (prf  2200))
(pw   ?pulse&:(>= ?pulse 6.5 ))
(pw   ?pulse&:(<= ?pulse 8.0))
(scan_rate ?call&:(>= ?call 3.5))
 (scan_rate ?call&:(<= ?call 4.0))
 =>

(printout t "This is AN/sps-58 low air-search
 radar" crlf))
(defrule signal-1-3
(freq ?x&:(>= ?x 5400))
(freq ?X&:(<= ?x 5600))
(prf  ?input&:(>= ?input 690))
(prf  ?input&:(<= ?input 800))
(pw   ?pulse&:(>= ?pulse 0.1))
```

```
(pw   ?pulse&:(<= ?pulse 0.5))
(scan_rate ?call&:(>= ?call 3.5))
(scan_rate ?call&:(<= ?call 4.5))
=>
(printout t " This is AN/sps-10 radar " crlf))

(defrule signal-1-4
(freq ?x&:(>= ?x 9100))
(freq ?x&:(<= ?x 9400))
(prf  ?input&:(>= ?input 1900))
(prf  ?input&:(<= ?input 2200))
(pw   ?pulse&:(>= ?pulse 0.1))
(pw   ?pulse&:(<= ?pulse 0.6))
(scan_rate ?call&:(>= ?call 3.0))
 (scan_rate ?call&:(<= ?call 4.2))
=>
(printout t " This is An/sps-65 radar" crlf))

(defrule signal-1-5
(freq ?x&:(>= ?x 2970))
(freq ?x&:(<= ?x 3020))
(prf  ?input&:(>= ?input 340))
(prf  ?input&:(<= ?input 410))
(pw   ?pulse&:(>= ?pulse 0.5))
(pw   ?pulse&:(<= ?pulse 1.2))
(scan_rate ?call&:(>= ?call 3.5))
(scan_rate ?call&:(<= ?call 4.5))
=>
(printout t "This is ??TYPE surface search radar
 " crlf))
(defrule signal-1-6
(freq ?x&:(>= ?x 9300))
(freq ?x&:(<= ?x 9450))
(prf  ?input&:(>= ?input 1800))
(prf  ?input&:(<= ?input 2150))
(pw   ?pulse&:(>= ?pulse 0.2))
(pw   ?pulse&:(<= ?pulse 0.5))
(scan_rate ?call&:(>= ?call 2.5))
(scan_rate ?call&:(<= ?call 4.5))
=>
(printout t "This is ?Type Fire control radar"
 crlf))
(defrule signal-1-7
(freq ?x&:(>= ?x 9300))
(freq ?x&:(<= ?x 9450))
(prf  ?input&:(>= ?input 3500))
(prf  ?input&:(<= ?input 4060))
```

```
(pw   ?pulse&:(>= ?pulse 0.2))
(pw   ?pulse&:(<= ?pulse 0.5))
(scan_rate ?call&:(>= ?call 2.0))
(scan_rate ?call&:(<= ?call 4.0))
=>
(printout t "This is a ?Type fire control radar"
 crlf))
(defrule signal-1-8
(freq ?x&:(>= ?x 9320))
(freq ?x&:(<= ?x 9501))
(prf  ?input&:(>= ?input 999.9999))
(prf  ?input&:(<= ?input 1000.9999))
(pw   ?pulse&:(>= ?pulse 0.1))
(pw   ?pulse&:(<= ?pulse 2.0))
(scan_rate ?call&:(>= ?call 2.0))
(scan_rate ?call&:(<= ?call 3.0))
=>
(printout t "This is ?Type Navigation radar"
 crlf))
(defrule signal-1-9
(freq ?x&:(>= ?x 9400))
(freq ?x&:(<= ?x 9490))
(prf  ?input&:(>= ?input 1000.1230))
(prf  ?input&:(<= ?input 1000.1239))
(pw   ?pulse&:(>= ?pulse 0.1))
 (pw   ?pulse&:(<= ?pulse 0.25))
(scan_rate ?call&:(>= ?call 2.0))
(scan_rate ?call&:(<= ?call 3.0))
=>
(printout t " This is ?Type Navigation radar
 "crlf))

(defrule input-1
=>
(printout t "Enter the following data: " crlf)
 (printout t crlf " frequency in MHZ :     " )
(assert (freq  =(read)))
(printout t crlf "    PRF in PPS      :     " )
(assert (prf   =(read)))
(printout t crlf " Pulse width in us :     " )
(assert (pw   =(read)))
(printout t crlf " Scan_rate in sec  :     " )
(assert (scan_rate  =(read))))
```

LIST OF REFERENCES

1. Schleher, D. Curtis, *Introduction to Electronic Warfare,* Artech House, Inc., Norwood, Massachusetts, 1986.

2. Griffiths, John, *Radio Wave Propagation and Antennas,* Prentice-Hall International (UK) Ltd, Englewood Cliff, New Jersey, 1987.

3. "Navy's EW Requirements Increasingly Critical," *ICH*, 1980.

4. Van Brunt, Leroy B., *Applied ECM*, 5th edition, Vol. 1, EW Engineering, Inc., Dunn Loring, Virginia, 1985.

5. Skolnik, Merrill I., *Introduction to Radar Systems*, McGraw-Hill, Inc., New York, 1980.

6. Hoisington, D. B., "Introduction to Electronic Warfare Handouts," Naval Postgraduate School, Monterey, California, 1990.

7. Wiley, Richard G., *The Analysis of Radar Signals*, Artech House, Inc., Norwood, Massachusetts, 1982.

8. Winston, Patrick H., *Artificial Intelligence*, 2nd edition, Addison-Wesley Publishing Co., Reading, Massachusetts, 1984.

9. Lehner, Paul E., *Artificial Intelligence and National Defense: Opportunity and Challenge*, Division of Tab Book, Inc., Blue Ridge Summit, Pennsylvania, 1989.

10. Jackson, Peter, *Introduction to Expert Systems*, 2nd edition, Addison-Wesley Publishing Co., Reading, Massachusetts, 1990.

11. Giarratano, Joseph C., *CLIPS User's Guide*, Vol. 4.3, Artificial Intelligence Section, Lyndon B. Johnson Space Center, 1989.

INITIAL DISTRIBUTION LIST

		No. of Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Chairman, Code EW Electronic Warfare Group Naval Postgraduate School Monterey, CA 93943-5000	1
4.	Professor Yuh-jeng Lee, Code CS/Le Department of Computer Sciences Naval Postgraduate School Monterey, CA 93943-5000	1
5.	Professor Donald v. Z. Wadsworth, Code EC/Wd Department of Electrical and Computer Engineering Naval Postgraduate School Monterey, CA 93943-5000	1
6.	LCdr. Hsiung Wen-Cheng, ROCN 18F, No. 40, GU00 Feng St., Tsoying KaoHsiung, TAIWAN, Republic of China	5

Thesis
H8296 Hsiung
c.1 A prototype rule based
system for electronic
warfare.